Avocent

CPS

Installer/User Guide

CPS810
CPS1610

INSTRUCTIONS

This symbol is intended to alert the user to the presence of important operating and maintenance (servicing) instructions in the literature accompanying the appliance.

DANGEROUS VOLTAGE

This symbol is intended to alert the user to the presence of uninsulated dangerous voltage within the product's enclosure that may be of sufficient magnitude to constitute a risk of electric shock to persons.

POWER ON

This symbol indicates the principal on/off switch is in the on position.

POWER OFF

This symbol indicates the principal on/off switch is in the off position.

PROTECTIVE GROUNDING TERMINAL

This symbol indicates a terminal which must be connected to earth ground prior to making any other connections to the equipment.

CPS810/1610
Installer/User Guide

USA Notification

Warning: Changes or modifications to this unit not expressly approved by the party responsible for compliance could void the user's authority to operate the equipment.

Note: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to Part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses and can radiate radio frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference in which case the user will be required to correct the interference at his own expense.

Canadian Notification

This digital apparatus does not exceed the Class A limits for radio noise emissions from digital apparatus set out in the Radio Interference Regulations of the Canadian Department of Communications.

Le présent appareil numérique n'émet pas de bruits radioélectriques dépassant les limites applicables aux appareils numériques de la classe A prescrites dans le Règlement sur le brouillage radioélectrique édicté par le Ministère des Communications du Canada.

Japanese Approvals

この装置は、情報処理装置等電波障害自主規制協議会（ＶＣＣＩ）の基準に基づくクラスA情報技術装置です。この装置を家庭環境で使用すると電波妨害を引き起こすことがあります。この場合には使用者が適切な対策を講ずるよう要求されることがあります。

Safety and EMC Standards

FCC P 15 Class A, EN55022, EN61000-3-2, EN61000-3-3, EN60950, EN55024, ETL (UL 1950), CSA 22.2 No. 950

This document is written for use with the CPS serial over IP network appliance application version 3.0 or later. References to DSView® management software apply to version 3.0 or later.

TABLE OF CONTENTS

List of Figures vii

List of Tables ix

Chapter 1: Product Overview 1

Features and Benefits 1

Safety Precautions 2

Using DSView Software 3

Chapter 2: Installation and Configuration 5

Hardware Overview 5

Installing the CPS Network Appliance 6

Configuring the CPS Appliance 7

Configuring the network addresses 7

Initial CPS appliance login 9

Reinitializing the CPS Network Appliance 10

Chapter 3: Operations 11

Overview 11

Configuring Serial Port Settings 11

Connecting to Serial Devices 13

Connecting to devices using Telnet 13

Connecting to devices from the serial CLI port 14

Configuring and using dial-in connections 15

Connecting to devices using PPP 15

Connecting to devices using SSH 16

Enabling plain text Telnet and SSH connections 19

Telnet CLI mode 20

Ending Device Sessions 20

Session time-out 21

Preemption 21

Managing User Accounts 22

Access rights and levels 23

Using Authentication Methods 24

Authentication of serial CLI port sessions 26
Authentication summary 26
Using security lock-out 27
Managing the Port History Buffer 28
Using port history mode commands 28
Managing the CPS Appliance Using SNMP 30
Chapter 4: Using CPS Appliance Commands 35
Accessing the CLI 35
Entering Commands 35
When commands take effect 36
Understanding Conventions 36
Command syntax 36
Syntax conventions 38
Command Summary 38
Chapter 5: CPS Appliance Commands 43
Connect Command 43
Disconnect Command 43
Help Command 44
Port Commands 44
Port Alert Add command 45
Port Alert Copy command 45
Port Alert Delete command 46
Port Break command 46
Port History command 46
Port Logout command 47
Port Set command 47
Port Set In/Out command 49
Quit Command 50
Resume Command 50
Server Commands 51
Server CLI command 51
Server FLASH command 53
Server Ping command 54

Server PPP command 54
Server RADIUS command 55
Server Reboot command 56
Server Security command 57
Server Set command 57
Server SNMP command 58
Server SNMP Community command 58
Server SNMP Manager command 59
Server SNMP Trap command 59
Server SNMP Trap Destination command 60
Server SSH command 61
Show Commands 62
Show Port command 62
Show Port Alert command 64
Show Port In|Out command 64
Show Server command 64
Show Server CLI command 65
Show Server PPP command 66
Show Server RADIUS command 66
Show Server Security command 66
Show Server SNMP command 67
Show User command 67
SPC Command 69
User Commands 70
User Add command 70
User Delete command 72
User Logout command 72
User Set command 72
User Unlock command 74
Appendices **75**
Appendix A: Technical Specifications 75
Appendix B: Device Cabling 77
Appendix C: Supported Traps 82
Appendix D: Ports Used 85

Appendix E: Technical Support *86*

Index **87**

LIST OF FIGURES

Figure 2.1: 16-port CPS Appliance Front Panel *5*
Figure 2.2: 16-port CPS Appliance Back Panel *6*
Figure B.1: CAT 5 Cable Adaptor Pin Assignments *78*
Figure B.2: Reversing Cable Adaptor Pin Assignments *80*
Figure B.3: 8-wire RJ-45 Reversing Cable *81*

LIST OF TABLES

Table 2.1: LEDs and Buttons 5
Table 3.1: Default Port Settings 11
Table 3.2: SSH Authentication Methods 17
Table 3.3: Access Rights 23
Table 3.4: Port History Mode Commands 28
Table 4.1: Line Editing Operations for VT100 Compatible Devices 35
Table 4.2: Line Editing Operations for ASCII TTY Devices 36
Table 4.3: Command Syntax Types in Example Command 36
Table 4.4: CPS Appliance Command Summary 38
Table 5.1: Connect Command Parameter 43
Table 5.2: Help Command Parameter 44
Table 5.3: Port Command Summary 44
Table 5.4: Port Alert Add Command Parameters 45
Table 5.5: Port Alert Copy Command Parameters 45
Table 5.6: Port Alert Delete Command Parameter 46
Table 5.7: Port Logout Command Parameter 47
Table 5.8: Port Set Command Parameters 48
Table 5.9: Port Set In/Out Command Parameters 50
Table 5.10: Server Command Summary 51
Table 5.11: Server CLI Command Parameters 52
Table 5.12: Server FLASH Command Parameters 53
Table 5.13: Ping Command Parameter 54
Table 5.14: Server PPP Command Parameters 55
Table 5.15: Server RADIUS Command Parameters 56
Table 5.16: Server Security Command Parameters 57
Table 5.17: Server Set Command Parameters 58

Table 5.18: Server SNMP Command Parameter 58
Table 5.19: Server SNMP Community Command Parameters 59
Table 5.20: Server SNMP Manager Command Parameters 59
Table 5.21: Server SNMP Trap Command Parameter 60
Table 5.22: Server SNMP Trap Destination Command Parameters 61
Table 5.23: Server SSH Command Parameters 61
Table 5.24: Show Command Summary 62
Table 5.25: Show Port Command Parameter 62
Table 5.26: Show Port Command Display Fields for Console Ports 63
Table 5.27: Show Port Command Display Fields for SPC Ports 63
Table 5.28: Show Port Alert Command Parameter 64
Table 5.29: Show Server Command Display Fields 64
Table 5.30: Show Server CLI Command Display Fields 65
Table 5.31: Show Server Security Command Display Fields 67
Table 5.32 Show User Command Parameter 68
Table 5.33: Show User Command Display Fields 68
Table 5.34: Show User All Command Display Fields 68
Table 5.35: SPC Command Parameters 69
Table 5.36: User Command Summary 70
Table 5.37: User Add Command 71
Table 5.38: User Delete Command Parameter 72
Table 5.39: User Logout Command Parameter 72
Table 5.40: User Set Command Parameters 73
Table 5.41: User Logout Command Parameter 74
Table A.1: CPS 810/1610 Appliance Technical Specifications 75
Table B.1: Port Pin Assignments 77
Table B.2: Adaptors for Use with CAT 5 Cable 77
Table B.3: Reversing Adaptors and Cables 79

Table C.1: CPS Appliance Enterprise Traps *82*
Table D.1: Ports Used by CPS Appliance *85*

CHAPTER 1

Product Overview

Features and Benefits

Overview

The CPS serial over IP network appliance provides non-blocked access and control for serial devices such as routers, power management devices and firewalls. This includes Avocent SPC power control devices that provide advanced power management and security.

You may connect up to 8 serial devices to a CPS810 appliance, and 16 serial devices to a CPS1610 appliance. A single 10/100 Ethernet port provides network connectivity. Two CPS appliances may be mounted in 1U of vertical space in a standard 19 inch rack.

Serial device access options

You may choose from among several available Telnet options to access the CPS network appliance and its attached serial devices:

- DSView® management software, which offers a built-in enhanced Telnet client
- Third party Telnet clients

Access to attached serial devices is also possible through a serial Command Line Interface (CLI) connection, a PPP (Point to Point Protocol) dial-in connection to a serial CLI modem or from a third party Secure Shell (SSH) client.

User authentication and data security

The CPS user database supports up to 64 user accounts, which include usernames, passwords and/or keys, plus specifications of access rights to CPS appliance ports and commands. User definitions may be changed at any time. You may choose to have user access authenticated locally at the CPS user database, at one or more DSView software servers or at one or more RADIUS (Remote Access Dial-In User Service) servers. Data security may be enhanced using industry-standard SSH encryption.

Extensive command set

The CPS network appliance offers a wide range of commands that allow administrators to easily configure, control and display information about the CPS appliance operating environment, including its ports, user accounts and active sessions. The user interface also offers descriptive

error message data and built-in command help information. On-board Trivial File Transfer Protocol (TFTP) support allows administrators to upload new functionality to CPS appliances in the field.

Port history

Each CPS port has a buffer that holds the most recent 64K bytes of online and offline serial data. A separate history command mode lets you navigate within a port's current history file and conduct tailored searches.

Safety Precautions

To avoid potential device problems when using Avocent products, if the building has 3-phase AC power, ensure that a computer and its monitor (if used) are on the same phase. For best results, they should be on the same circuit.

To avoid potentially fatal shock hazard and possible damage to equipment, please observe the following precautions:

- Do not use a 2-wire extension cord in any Avocent product configuration.
- Test AC outlets at the computer and monitor (if used) for proper polarity and grounding.
- Use only with grounded outlets at both the computer and monitor. When using a backup Uninterruptible Power Supply (UPS), power the computer, the monitor and the CPS appliance off the supply.

NOTE: The AC inlet is the main disconnect.

Rack mount safety considerations

- Elevated Ambient Temperature: If installed in a closed rack assembly, the operation temperature of the rack environment may be greater than room ambient. Use care not to exceed the rated maximum ambient temperature of the unit.
- Reduced Airflow: Installation of the equipment in a rack should be such that the amount of airflow required for safe operation of the equipment is not compromised.
- Mechanical Loading: Mounting of the equipment in the rack should be such that a hazardous condition is not achieved due to uneven mechanical loading.
- Circuit Overloading: Consideration should be given to the connection of the equipment to the supply circuit and the effect that overloading of circuits might have on overcurrent protection and supply wiring. Consider equipment nameplate ratings for maximum current.
- Reliable Earthing: Reliable earthing of rack mounted equipment should be maintained. Pay particular attention to supply connections other than direct connections to the branch circuit (for example, use of power strips).

Using DSView Software

The DSView management software may be used to manage CPS appliances and access attached devices. Using DSView software, you may perform most of the operations that are described in this manual. This manual describes how to manage a CPS appliance by entering commands using the CLI. The DSView Installer/User Guide describes how to manage a CPS appliance using the DSView software graphical interface.

CHAPTER 2

Installation and Configuration

Hardware Overview

Figure 2.1 shows the front panel of a 16-port CPS network appliance.

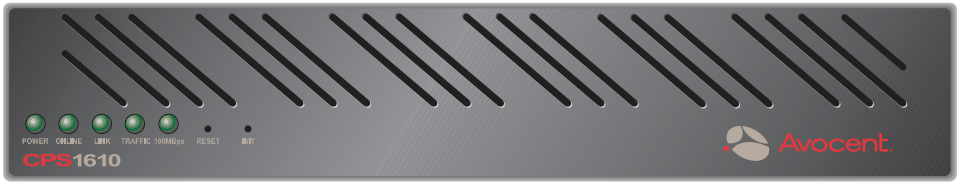


Figure 2.1: 16-port CPS Appliance Front Panel

The lower left area of the front panel contains five LEDs and two buttons, which are described in Table 2.1.

Table 2.1: LEDs and Buttons

LED/Button	Description
POWER	The *POWER* LED illuminates when the CPS appliance is connected to a power source.
ONLINE	The *ONLINE* LED illuminates steadily (not blinking) when the CPS self-test and initialization procedures complete successfully.
LINK	The *LINK* LED illuminates when the CPS appliance establishes a connection to the network.
TRAFFIC	The *TRAFFIC* LED blinks when there is network traffic.
100MBps	The *100MBps* LED illuminates when the CPS appliance is connected to a 100 MBps LAN.
RESET	The RESET button, when pressed, reboots the CPS appliance.
INIT	The INIT button, when pressed and held, restores the CPS appliance to factory defaults; for more information, see *Reinitializing the CPS Network Appliance* on page 10.

As shown in Figure 2.2, the back of the CPS appliance contains RJ-45 connectors for serial cabling (8 connectors for an 8-port CPS appliance model or 16 connectors for a 16-port CPS appliance), a LAN connector for a 10BaseT or 100BaseT interface cable and a power receptacle.

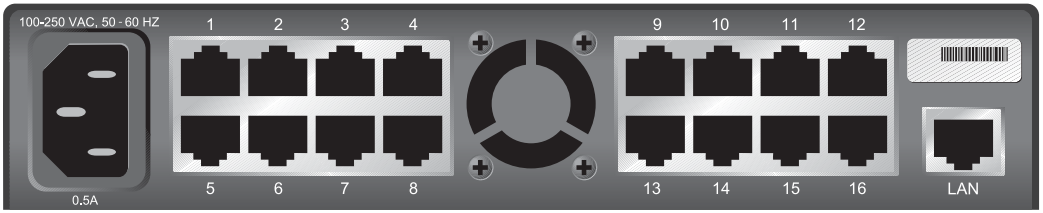


Figure 2.2: 16-port CPS Appliance Back Panel

Installing the CPS Network Appliance

WARNING: The power outlet should be near the equipment and easily accessible.

To install the CPS appliance hardware:

1. Place the unit where you can connect cables between the serial devices and the CPS serial ports, and where you can connect a LAN interface cable between the Ethernet hub or switch and the CPS LAN connector.

   If you are using a rack mount kit, follow the instructions included with the kit.
2. Connect serial devices to the CPS serial ports; see *Device Cabling* on page 77 for cable information. Connect each serial device to its appropriate power source, following the device's documentation.
3. Attach a 10BaseT or 100BaseT LAN interface cable to the LAN connector on the back of the CPS appliance. A CAT 5 cable is required for 100BaseT operation.
4. Insert the power cord into the back of the unit. Insert the other end of the power cord into a grounded electrical receptacle.
5. Check that the *POWER* LED is illuminated. If not, check the power cable to ensure that it is inserted snugly into the back of the unit. The *ONLINE* LED will illuminate within one minute to indicate that the self-test is complete. If the *ONLINE* LED blinks, contact Avocent Technical Support for assistance.
6. Check that the *LINK* LED is also illuminated. If not, check the Ethernet cable to ensure that both ends are correctly inserted into their jacks. If the unit is not correctly connected to an Ethernet hub or switch, you will not be able to configure the appliance for operation. If the unit is connected to a 100 MB Ethernet hub, the *100MBps* LED will also be illuminated.
7. Once the *POWER*, *ONLINE* and *LINK* LEDs are illuminated, proceed with the configuration process. (If you will be configuring the network address information with BootP, remove power from the CPS appliance.)

WARNING: The CPS appliance and all attached devices should be powered down before servicing the unit. Always disconnect the power cord from the wall outlet.

Configuring the CPS Appliance

To configure the CPS network appliance, you must specify a unique IP address, plus other network address information. This information will be stored in the CPS configuration database. During initial login, you will specify a password for the Admin user.

Configuring the network addresses

You may use any of four methods to configure the network information: DSView software, BootP, Telnet Command Line Interface (CLI) or the serial CLI on port 1.

These methods work as documented on most Windows and UNIX systems; however, the actual implementation on your system may differ from the instructions provided. Refer to your system administrator guide.

To configure the network addresses using DSView software:

Using the DSView software installation wizard is the easiest method to configure the CPS appliance IP address, subnet mask and gateway. See the DSView Installer/User Guide for instructions. After the network addresses are configured, see *Initial CPS appliance login* on page 9.

To configure the network addresses using BootP:

1. Ensure that there is a BootP server on your network that is configured to correctly respond to a BootP request from the CPS appliance. BootP servers require the Ethernet MAC address of network devices. The Ethernet MAC address is located on the back panel above the LAN connector. See your BootP server's system administrator guide for information about configuring the BootP server.
2. After you have configured your network's BootP server with the CPS appliance Ethernet MAC address, IP address, subnet mask and gateway, restore power to the CPS appliance and wait for the *ONLINE* LED to illuminate. Once this occurs, the CPS appliance has completed the BootP protocol, obtained its IP address and subnet mask and stored these in FLASH.
3. You may verify that the BootP process was successful with a ping command, which tests network connectivity. The ping command is entered as:

   ```
   ping <ip_address>
   ```

   For example, the following command tests the network connectivity of a CPS appliance with the IP address 192.168.0.5.

   ```
   ping 192.168.0.5
   ```

4. If the CPS network appliance completes the BootP successfully, you will see a display similar to the following.

   ```
   Pinging 192.168.0.5 with 32 bytes of data:
   ```

```
Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
Reply from 192.168.0.5: bytes=32 time<10ms TTL=128
```

If the CPS appliance did not successfully obtain its IP address with the BootP protocol, you will see a display similar to the following.

```
Pinging 192.168.0.5 with 32 bytes of data
Request timed out.
Request timed out.
Request timed out.
Request timed out.
```

In this case, check the addresses provided to the BootP server to confirm they are correct. Verify that the Ethernet LAN adaptor cable is correctly installed on the CPS appliance and the Ethernet hub.

After the network addresses are configured successfully, launch a Telnet session to the assigned IP address. Then, see *Initial CPS appliance login* on page 9.

To configure the network addresses using a Telnet CLI:

1. Ensure that your server or workstation has a Telnet client and is located on the same LAN segment as the CPS network appliance.
2. Use the arp command to update the server or workstation with the IP address and Ethernet MAC address. The Ethernet MAC address is located on the back panel above the LAN connector. The arp command is entered as:

   ```
   arp -s <ip_address> <mac_address>
   ```

   For example, the following command assigns the IP address 192.168.0.5 and the Ethernet MAC address 00-80-7d-54-01-54 to the CPS appliance.

   ```
   arp -s 192.168.0.5 00-80-7d-54-01-54
   ```

   On a UNIX platform, the MAC address may require colons (:) instead of dashes (-), for example, 00:80:7d:54:01:54.
3. You may verify that you entered the information correctly by using an arp command with the -a option.

   ```
   arp -a
   ```

   This command shows all arp entries for the server or workstation. See your system administrator guide if you need additional help with the arp command.
4. After the above arp command is entered correctly, launch a Telnet client to the assigned IP address. Then, continue with *Initial CPS appliance login* on page 9.

To configure the CPS appliance using the serial CLI:

1. By factory default, port 1 of the CPS appliance is configured for the serial CLI. To access the serial CLI, attach a compatible device to port 1. The compatible device types are: ASCII, VT52, VT100, VT102, VT220 and VT320.

For cable and adaptor information, see *Device Cabling* on page 77. You may also use any terminal emulation program that is available on your system.

2. Configure your terminal or terminal emulation program as follows.

Baud rate	9600
Bits per character	8
Stop bits	1
Flow control	None

3. Press the **Return** or **Enter** key until a prompt appears, requesting your username. If you do not receive a prompt after pressing the key five times, check your cable and serial settings to be sure that they are correct.
4. Proceed to *Initial CPS appliance login* on page 9.

After you complete the CPS appliance configuration, you may reconfigure the CLI on another port or disable it completely and use port 1 with an attached device. For more information, see *Connecting to devices from the serial CLI port* on page 14.

Initial CPS appliance login

The CPS appliance ships with a single user defined in its user database. This predefined user has the name Admin, no password and has the Appliance Administrator access level. The first time you connect to the CPS network appliance, you are prompted for a username.

To log in to the CPS appliance for the first time:

1. At the Username prompt, type **Admin**. There is no factory default password for the Admin user. At the Password prompt, press **Return**.

```
Avocent CPS16xx S/W Version x.x (ASCII)
Username: Admin
Password:
Authentication Complete
CPS configuration is required.
```

2. Once authentication completes, the CPS appliance prompts for any missing configuration values that are required for operation.

   If you already provided the IP address, subnet mask and gateway, you will not be prompted for those values again.

   If you have not already provided the network information, you will be prompted for them. Enter the addresses using standard dot notation.

```
CPS configuration is required
Enter CPS IP address > 192.168.0.5
Enter CPS Subnet mask > 255.255.255.0
Enter CPS Gateway address > 0.0.0.0
```

3. You are prompted for a new Admin password. Passwords are case sensitive and must contain 3-16 alphanumeric characters. You must enter the new password twice to confirm that you entered it correctly.

```
Enter CPS New Admin Password > *****
Confirm New Admin Password > *****
```

After you have provided the required configuration information, a confirmation message appears while the CPS appliance stores the values in its configuration database.

You have now completed the initial login, and you may enter additional commands at the CLI prompt (>). To configure other CPS appliance ports, see *Configuring Serial Port Settings* on page 11.

Reinitializing the CPS Network Appliance

Reinitializing the CPS appliance removes configured information. This may be useful when reinstalling the unit at another location in your network.

The CPS appliance stores configuration information in FLASH databases. During reinitialization, the FLASH erase has two phases. The first phase erases the configuration database, which contains all nonvolatile data except the IP address. The second phase erases the IP address and restores the CPS appliance to its factory default settings.

To reinitialize the CPS appliance:

1. Locate the recessed INIT button on the front of the CPS appliance. An opened paper clip may be used to depress the button.
2. Insert the end of the opened paper clip in the recess, then depress and hold the button. The *ONLINE* LED will blink, indicating an initialization has been requested. You have approximately seven seconds to release the button before any action is taken.

   After seven seconds, the *ONLINE* LED will blink more rapidly to confirm that the CPS configuration database has been erased. Continuing to hold the INIT button for a few more seconds will erase the IP address as well. The *ONLINE* LED will blink faster to confirm the deletion.

If any portion of FLASH is erased, the CPS appliance reboots when the INIT button is released.

You may also use the Server FLASH command to update the CPS FLASH application or boot program. For more information, see *Server FLASH command* on page 53.

CHAPTER 3

Operations

Overview

The CPS serial over IP network appliance and its ports are easily configured and managed to meet your requirements for device connection, user authentication, access control, power status monitoring, port history information display and Simple Network Management Protocol (SNMP) compliance for use with third party network management products. Support for SSH access using third party clients is also provided.

Configuring Serial Port Settings

You may configure a CPS port to support one of two types of target devices (TDs): SPC and console. The SPC power control device provides enhanced security options, including password protection, port-specific access rights and port groupings. For more information, see the SPC Installer/User Guide. A console TD may be a router, firewall, server or other supported serial device.

By default, ports are configured with the settings listed in Table 3.1.

Table 3.1: Default Port Settings

Parameter	Value
Target device	Console
Name	xx-xx-xx Pn (last 3 octets of MAC address plus the port number)
Baud rate	9600
Bits per character	8
Parity	None
Stop bits	1
Flow control	None
Time-out	15 minutes
CLI access character	User Server CLI setting (^D)

Table 3.1: Default Port Settings (Continued)

Parameter	Value
Power	None

Most of these settings are standard serial port operating characteristics.

The CLI access character parameter specifies how you access the CLI. For more information, see *Telnet CLI mode* on page 20.

The Power parameter instructs the CCM appliance to monitor the state of a specified control signal. Signal transitions may be configured to trigger SNMP traps. The parameter value indicates an inbound control signal (CTS, DCD or DSR) and the state of that signal (low or high). When the defined signal is true, the CPS appliance interprets it as a power on condition for the attached device; when the signal is false, a power off condition for the device is assumed. The signal specified for flow control may not be used for power control, and vice versa.

To configure serial console port settings:

Issue a Port Set command. You may specify settings for one or all ports.

PORT [<*port*>|ALL] SET TD=CONSOLE [NAME=<*name*>] [BAUD=<*baud*>] [SIZE=<*size*>] [PARITY=<*parity*>] [STOP=<*stop_bits*>] [FLOW=<*flow_ctrl*>] [TIMEOUT=<*time-out*>] [SOCKET=<*socket*>] [CHAR=^<*cli_char*>] [TOGGLE=NONE|DTR] [POWER=<*signal*>]

To configure SPC ports and settings:

Issue a Port Set command with the TD=SPC parameter.

PORT <*port*> SET TD=SPC

When a port is configured as an SPC, you cannot change the serial port settings. However, you may use the SPC command to change certain configuration values for the SPC and its individual sockets.

SPC <*port*>|ALL [MINLOAD=<*amps*>] [MAXLOAD=<*amps*>] [SOCKET <*socket*>|ALL] [WAKE=ON|OFF] [ONMIN=<*time*>] [OFFmin=<*time*>]

For more information, see *Port Set command* on page 47 and *SPC Command* on page 69.

When you specify TD=SPC, you may configure the SPC device and control its individual sockets using DSView software. Existing users who already have an SPC device and use its native command interfaces should specify TD=Console.

To display serial port settings:

Issue a Show Port command.

SHOW PORT [<*port*>|ALL|NAMES]

When you request information about a console port, the display includes configuration information, current power status (if power status monitoring has been enabled), plus transmit, receive and error counts. When you request information about a single console port and a user is currently accessing

that port, the display also includes the username, access rights and other information about the current session.

When you request information about a single SPC port, the display includes information configured with the SPC command. A Show Port All command will indicate which ports are SPC ports.

When you request information about port names, the display includes the port numbers and names. If a port's name has not been changed with a Port Set command, the logical name is displayed.

For more information, see *Show Port command* on page 62.

Connecting to Serial Devices

The CPS network appliance offers several methods for connecting to attached serial devices: Telnet, serial CLI, PPP and SSH.

Connecting to devices using Telnet

Each CPS serial port is directly addressable through a unique TCP port that provides a connection to the attached serial device. You may connect using either SSH or plain text.

DSView management software

The Avocent DSView management software offers an interface to access devices attached to Avocent digital Keyboard, Video and Mouse (KVM) appliances and CPS network appliances. The Telnet client built into the DSView software uses Windows server-based authentication and authentication servers to control access. Third party Telnet clients may also be supported with DSView management software. For more information, see the DSView Installer/User Guide.

Standalone third party Telnet clients

You may use third party Telnet clients to access the CPS appliance directly without DSView management software.

To connect to a device using Telnet:

Type **telnet,** followed by the CPS IP address and the appropriate TCP port, which by default is 3000 plus the physical port number, in decimal format. (The TCP port number may be changed for any CPS port.)

For example, the following Telnet command connects to the serial device attached to physical port 14 of the CPS network appliance.

```
telnet 192.168.0.5 3014
```

If an authentication method other than None has been configured for the CPS appliance, you will be prompted for a username and password. Once authentication completes, your connection is confirmed. When you successfully connect to the serial device, you will see a display similar to the following.

```
Avocent CPS ...
Username: Myname
Password: ******
```

```
Authentication Complete
Connected to Port: ...
```

If the authentication method is configured as None, you may Telnet and connect to a serial device without entering credentials; however, credentials are always required when connecting to the CPS CLI.

Data entered at the Telnet client is written to the attached serial device. Any data received by the CPS appliance from the serial device is output to your Telnet client.

Connecting to devices from the serial CLI port

By factory default, port 1 of the CPS network appliance is configured with the serial CLI, which prohibits the use of port 1 with an attached serial device. You may configure the CLI on a different port, but only one port may be configured as the serial CLI port at one time. For example, if you attempt to enable the CLI interface on port n, and it is already active on port p, then the CLI will automatically be disabled on port p.

You may connect to one serial device at a time through the serial CLI port using a local terminal or a local PC using a terminal emulation program. If you connect an external modem to the serial CLI port, you may also access devices through a remote terminal or PC that can dial into the external modem. For information about modem connections, see *Connecting to devices using SSH* on page 16, *Configuring and using dial-in connections* on page 15 and *Server CLI command* on page 51.

For more information about serial CLI port connections, see *Authentication of serial CLI port sessions* on page 26 and *Preemption* on page 21.

To configure a port for the serial CLI:

1. Issue a Server CLI command, using the Port parameter to specify the CLI port and the Type parameter to specify the terminal type.

   SERVER CLI PORT=<*port*> TYPE=<*type*>

2. To disable the CLI that was previously configured on a port, issue a Server CLI command, indicating Type=Off.

For more information, see *Server CLI command* on page 51.

To display CLI port information:

Issue a Show Server CLI command.

SHOW SERVER CLI

The display includes the CLI port number and terminal type, plus the CLI access character. For more information, see *Show Server CLI command* on page 65.

To connect to a device from the serial CLI port:

1. Issue a Server CLI command, using the Connect parameter to enable the use of the Connect command from the serial CLI port.

   ```
   SERVER CLI CONNECT=ON
   ```

2. Issue a Connect command to the desired port.

   CONNECT <*port*>

3. To end a device session that was initiated with a Connect command, issue a Disconnect command.

   DISCONNECT

For more information, see *Server CLI command* on page 51, *Connect Command* on page 43 and *Disconnect Command* on page 43.

Configuring and using dial-in connections

You may attach an external modem to the serial CLI port for dial-in serial CLI access to the CPS appliance. This may be used as a backup connection if the unit is not accessible from the network. It may also be used as a primary connection at remote sites that do not have Ethernet network capability. The modem must be Hayes compatible.

To specify a modem initialization string:

1. Issue a Show Server CLI command to ensure that the port where the modem is connected has been defined as the serial CLI port.

   SHOW SERVER CLI

2. Issue a Server CLI command, using the Modeminit parameter to specify the modem initialization string.

   SERVER CLI MODEMINIT="<*string*>"

   The string must be enclosed in quotes and must include at least the command settings ATV1 and SO=1, which cause the modem to issue verbose response strings and auto-answer the phone on the first ring. For more information, see *Server CLI command* on page 51.

   The modem initialization string is sent to the cabled modem when any of the following conditions occur:

   - CPS appliance initialization
   - Detection of a transition of DSR from low to high
   - Completion of a call when DCD changes from high to low

3. Upon successful modem connection, press the **Enter** key until the login prompt appears.

To display modem configuration information:

Issue a Show Server CLI command.

SHOW SERVER CLI

For more information, see *Show Server CLI command* on page 65.

Connecting to devices using PPP

The CPS network appliance supports remote PPP access using an auto-answer modem that answers calls and establishes the PPP protocol with a dial-in client.

The PPP dial-in may be used to access a remote CPS appliance that does not warrant a WAN (Wide Area Network) link to the Ethernet interface. In this case, the PPP connection allows a remote PC with Telnet capability to dial the CPS appliance and then establish a Telnet connection to a port.

The PPP dial-in may also be used to access a subnet containing remote CPS devices in the event of a WAN link failure. In this case, the PPP provides an alternate path to one or more remote CPS devices.

Once the PPP connection is established, you must launch an application that connects to the CPS appliance or to one of its ports. The PPP connection is only a communications interface to the CPS appliance.

The CPS appliance implements a PPP server that uses CHAP (Challenge Authentication Protocol). Passwords are not accepted in the clear on PPP connections.

The authentication of PPP dial-in connections is not affected by enabling/disabling the server-level CLI port authentication parameter. See *Preemption* on page 21 for more information.

To enable or disable a PPP server on the serial CLI port:

1. To enable a PPP server on the serial CLI port, issue a Show Server CLI command to ensure that a serial CLI port has been defined.

   SHOW SERVER CLI

2. Issue a Server PPP command with the Enable parameter.

   SERVER PPP ENABLE LOCALIP=<*local_ip*> REMOTEIP=<*rem_ip*> [MASK=<*subnet*>]

   You must specify local and remote IP addresses to be used for the CPS appliance and client ends of the PPP connection respectively. You are prompted to confirm or cancel the changes. Enter **Y** to confirm or **N** to cancel.

3. To disable a PPP server, issue a Server PPP command with the Disable parameter.

   SERVER PPP DISABLE

For more information, see *Show Server CLI command* on page 65 and *Server PPP command* on page 54.

To display PPP configuration information:

Issue a Show Server PPP command.

SHOW SERVER PPP

For more information, see *Show Server PPP command* on page 66.

Connecting to devices using SSH

The CPS serial over IP network appliance supports version 2 of the SSH protocol (SSH2). The CPS SSH server operates on the standard SSH port 22. The shell for this connection provides a CLI prompt as if you had established a Telnet connection on port 23. The shell request for this connection is for CLI access.

Additional CPS SSH servers operate on TCP ports that are numbered with values 100 greater than the standard 30xx Telnet ports for the CPS appliance. For example, if port 7 is configured for

Telnet access on port 3007, then port 3107 will be a direct SSH connection for port 7. When SSH is enabled, Telnet port 23 connections will be accepted from other clients if the Server Security command includes the Encrypt=SSH,None parameter, which indicates that both SSH and plain text connections will be allowed. Connecting to Telnet port 23 may also be tunneled through a connection to SSH port 22.

Telnet, DSView software and SSH clients may authenticate using a DS server.

SSH server keys

When SSH is enabled for the first time, the CPS generates an SSH server key. The key generation process may take up to ten minutes. The key is computed at random and is stored in the CPS configuration database.

In most cases, the SSH server key should not be modified because most SSH clients will associate the key with the IP address of the CPS appliance. During the first connection to a new SSH server, the client will display the SSH server's key. You will be prompted to indicate if it should be stored on the SSH client. After the first connection, most SSH clients will validate the key when connecting to the CPS appliance. This provides an extra layer of security because the SSH client can verify the key sent by the server each time it connects.

When you disable SSH and later reenable it, you may either use the existing server key or compute a new one. If you are reenabling the same server at the same IP address, it is recommended that you use the existing key, as SSH clients may be using it for verification. If you are moving the CPS appliance to another location and changing the IP address, you may wish to generate a new SSH server key.

Authenticating an SSH user

SSH is enabled and disabled with the Server SSH command. When you enable SSH, you may specify the authentication method(s) that will be used for SSH connections. The method may be a password, an SSH key or both. A user's password and SSH key are specified with a User Add or User Set command. All SSH keys must be RSA keys. DSA keys are not supported.

Table 3.2 lists and describes the valid SSH authentication methods that may be specified with a Server SSH command.

Table 3.2: SSH Authentication Methods

Method	Description
PW (default)	SSH connections will be authenticated with a username/password. With this method, a user's definition must include a valid password in order for that user to authenticate an SSH session. A password may authenticate to a DSView software or RADIUS server or to the local user database.
KEY	SSH connections will be authenticated with an SSH key. With this method, a user's definition must include valid SSH key information in order for that user to authenticate an SSH session. Key authentication is always local; RADIUS is not supported. For more information, see *SSH user keys* on page 18.

Table 3.2: SSH Authentication Methods (Continued)

Method	Description
PW|KEY or KEY|PW	SSH connections will be authenticated with either a username/password or an SSH key. If a user has only a password defined, that user must authenticate an SSH session with a username/password. If a user has only an SSH key defined, that user must authenticate an SSH session using the key. If a user has both a password and an SSH key defined, that user may use either a username/password or the SSH key to authenticate an SSH session. This method allows the administrator to define how each user will authenticate an SSH session based on information provided in the User Add/Set command. PW authentication will be local, RADIUS or DS as specified in the Auth parameter of the Server Security command. Key authentication is always local.
PW&KEY or KEY&PW	SSH connections will be authenticated using both a username/password and an SSH key. With this method, a user's definition must include a password and SSH key information for that user to authenticate an SSH session. PW authentication will be local, RADIUS or DS as specified in the Auth parameter of the Server Security command. Key authentication is always local.

A user's access rights are determined from the authentication method used. SSH key authentication always uses the access rights from the local user database. Depending on the server authentication method specified with the Server Security command, SSH password authentication will use either the access rights from the local user database, the DSView software server or the values returned by the RADIUS server.

With either of the "or" methods (PW|KEY and KEY|PW), the user access rights are determined from the method used to authenticate the user.

With either of the "and" methods (PW&KEY and KEY&PW), the user access rights are determined from the first method specified. If PW&KEY is specified, the access rights from the password authentication will be used. If KEY&PW is specified, the access rights from the key authentication will be used.

For more information, see *Using Authentication Methods* on page 24.

SSH user keys

A user's SSH key is specified in a User Add or User Set command. You may define a key even if SSH is not currently enabled. The key may be specified in one of two ways:

- When using the SSHKEY and FTPIP keyword pair to define the network location of a user's SSH key file, the SSHKEY parameter specifies the name of the uuencoded (Unix to Unix encoded) public key file on an FTP server. The maximum file size that can be received is 4K bytes. The FTPIP parameter specifies the FTP server's IP address.

  When this method is specified, the CPS appliance initiates an FTP client request to the specified IP address. The CPS appliance then prompts the user for an FTP username and password for connection. When connected, the CPS appliance will GET the specified key file

and the FTP connection will be closed. The CPS appliance then stores the SSH key with the username in the CPS user database.

- When using the KEY keyword to specify the SSH key, the KEY parameter specifies the actual uuencoded SSH key. This is for configurations that do not implement an FTP server. The CPS appliance stores the specified key in the CPS user database.

The CPS appliance processes a uuencoded SSH2 public key file with the format described in the IETF document draft-ietf-secshpublickeyfile-02. The key must follow all format requirements. The UNIX ssh-keygen2 generates this file format. The CPS appliance also processes a uuencoded SSH1 public key file. The UNIX ssh-keygen generates this file format.

To enable SSH session access to the CPS network appliance:

1. Issue a Show Server Security command to ensure that you are using an authentication method other than None.

   SHOW SERVER SECURITY

2. Issue a Server SSH command with the Enable parameter. You may also specify an authentication method.

   SERVER SSH ENABLE AUTH=<*auth*>

   If an authentication method is not specified, the previous authentication parameter will be used. The default value is AUTH=PW.

3. If you are enabling SSH for the first time, you are advised that all other CPS appliance sessions will be terminated. Enter **Y** to continue or **N** to cancel.

4. If you are reenabling SSH, you are prompted to use the existing SSH server key or generate a new key. Enter **Y** to use the existing key or **N** to generate a new key.

For more information, see *Server SSH command* on page 61.

To disable SSH session access to the CPS appliance:

Issue a Server SSH command with the Disable parameter.

SERVER SSH DISABLE

When SSH is disabled, the CPS appliance operates in plain text mode.

To display SSH information:

Issue a Show Server Security command.

SHOW SERVER SECURITY

If SSH is enabled, the display will include SSH2. Regardless of whether SSH is enabled, the display will indicate the authentication method that was specified with the Server SSH command.

Enabling plain text Telnet and SSH connections

Plain text (non-encrypted) Telnet connections are enabled by default.

If you enable SSH connections using the Server Security command with the Encrypt=SSH parameter, plain text Telnet connections will be disabled. However, if you enable SSH connections with the Server SSH command, both plain text and SSH connections will be allowed.

To enable both Telnet and SSH connections:

Issue a Server Security command, indicating Encrypt=SSH,None.

Telnet CLI mode

While you are connected to an attached serial device, you may enter Telnet CLI mode and enter CPS appliance commands.

To enter or exit CLI mode when connected to a serial device:

1. To enter CLI mode, type the CLI access character, which is **Ctrl-D** by default. At the CLI prompt (>), you may enter CPS commands.
2. To exit CLI mode and return to the session with the attached device, issue a Resume command.

   RESUME

For more information, see *Resume Command* on page 50.

To change the CLI access character:

Issue a Server CLI command or a Port Set command, using the Char parameter to specify the CLI access character.

SERVER CLI CHAR=^<*char*>
- or -
PORT SET CHAR=^<*char*>

If you issue a Port Set command with Char=None, then the CLI access character specified in the Server CLI command will be used. You may use the Port Set command to override the Server CLI access character on a per-port basis.

For more information, see *Server CLI command* on page 51 and *Port Set command* on page 47.

To display CLI access character information:

Issue a Show Server CLI command.

SHOW SERVER CLI

For more information, see *Show Server CLI command* on page 65.

Ending Device Sessions

To end your session:

Enter CLI mode and issue a Quit command.

QUIT

- or -

If you initiated the device session with a Connect command, enter CLI mode and issue a Disconnect command.

DISCONNECT

- or -

Allow the port to time-out due to inactivity. In this case, a notification message is issued and the serial CLI session returns to CLI mode. This time-out may occur while you are in CLI mode.

- or -

For modem connections, if a carrier drop occurs, the serial CLI session is automatically logged off.

For more information, see the *Quit Command* on page 50 and the *Disconnect Command* on page 43.

To end another user's session:

Issue a User Logout command.

USER LOGOUT <*username*>

A message is sent and the Telnet or SSH connection is dropped.

For more information, see *User Logout command* on page 72. For information about preempting a user's session, see *Connecting to devices using Telnet* on page 13.

Session time-out

The CPS appliance monitors data traffic when you are connected to an attached serial device. You may specify a time-out value with the Server CLI command. You may also specify a time-out value for each port with the Port Set command. When no data is received from the connected user for the configured number of minutes, the connection is terminated.

The following time-out values are used:

- For a Telnet session, the Server CLI time-out value is used.
- For a serial port session, if the port's configured time-out value is zero, the Server CLI time-out value is used, even if it is also zero.
- For a serial port session, if the port's configured time-out value is non-zero, that value is used.

Preemption

Configured preemption levels determine whether a user who wishes to connect to a port (the connecting user) may preempt another user who is already using that port (the current user). Preemption levels are configured for each user with the User Add or User Set commands. Preemption levels range from one to four. Four is the highest level and is also the default.

- If the connecting user's preemption level is lower than the current user's preemption level, the connecting user will receive an *In Use* message and the connection will be dropped.
- If the connecting user's preemption level is equal to or higher than the owning user's preemption level, an *In Use by owning user* message will be displayed. The connecting user may then choose to preempt the current user's session. If the current user's session is preempted, an appropriate message is displayed.

A server-level preemption level may also be configured with the Server CLI command. This value is used when authentication is disabled on the serial CLI port and a user on that port attempts to connect to another port that is already in use.

For example, assume authentication has been disabled on the serial CLI port. A user starts a session on the serial CLI port (without having to log in with a username and password), then attempts to connect to port 7, which is already in use by another user. Since the CLI port user's preemption level is not known (because no authentication occurred during login), the configured server-level preemption level is used.

- If that preemption level is lower than the current port 7 user's preemption level, the connection to port 7 will not be allowed.
- If that preemption level is equal to or higher than the current port 7 user's preemption level, the serial CLI port user may choose to preempt the current port 7 user's session.

NOTE: Even if authentication is disabled on the CLI port, PPP sessions will be authenticated using the settings configured with the Server Security command. Enabling/disabling serial port CLI session authentication does not apply to PPP dial-in connections.

For more information, see *Authentication of serial CLI port sessions* on page 26.

Managing User Accounts

The CPS user database can store information for up to 64 user accounts.

To add a user:

Issue a User Add command.

USER ADD <*username*> [PASSWORD=<*pwd*>] [SSHKEY=<*keyfile*>] [FTPIP=<*ftpadd*>] [KEY=<*sshkey*>] [ACCESS=<*access*>]

You must specify a username. You must also specify a password or SSH user key information, or you may specify both. You may also include an access level or access rights. For more information, see *Connecting to devices using SSH* on page 16, *Access rights and levels* on page 23 and *User Add command* on page 70.

To change a user's configuration information:

Issue a User Set command.

USER SET <*username*> [PASSWORD=<*pwd*>] [SSHKEY=<*keyfile*>] [FTPIP=<*ftpadd*>] [KEY=<*sshkey*>] [ACCESS=<*access*>]

You may change your own password at any time. You must have USER access rights to change another user's password or to change any user's SSH user key information and access rights.

To remove an SSH user key or password, specify Key="" or Password="". You cannot remove both the password and the SSH key from a user's definition; one must remain in the user database. Also, you cannot remove a user's key or password if that removal would result in no valid users having USER access rights.

For more information, see *Connecting to devices using SSH* on page 16, *Access rights and levels* on page 23 and *User Set command* on page 72.

To delete a user:

Issue a User Delete command.

USER DELETE <*username*>

If the specified user is currently logged in, a message is sent to the user indicating that access is no longer permitted, and the user's Telnet session is terminated. For more information, see *User Delete command* on page 72.

To display user configuration information:

1. To display information about one user, issue a Show User command, specifying the username.
   SHOW USER <*username*>
2. To display information about all users, issue a Show User command with the All parameter.
   SHOW USER ALL

For more information, see *Show User command* on page 67.

Access rights and levels

Most CPS appliance commands require the user to have access rights to use the commands. The access rights for each command are listed in Table 4.4 on page 38. Table 3.3 describes the access rights a user may be given.

Table 3.3: Access Rights

Access Right	Description
PCON	The Port Configuration access right allows the user to modify port settings. Grant PCON access only to users who need to issue the Port Set command.
SCON	The Server Configuration access right allows the user to change the CPS configurations, including setting the IP address and updating the program load in FLASH. Grant SCON access only to users who need to administer the CPS appliance.
SMON	The Server Monitor access right allows the user to view CPS appliance status and monitor serial port activity. Grant SMON access only to users who need to assist other users in accessing attached serial devices.
USER	The USER access right allows the user to modify the user database. Grant USER access only to users who need to add users, change user specifications or delete users. At least one user must have USER access rights; otherwise, the user database cannot be changed.
BREAK	The BREAK access right allows the user to send a serial break sequence to the attached serial device. On certain devices, this sequence has a special meaning. Grant BREAK access only to users who need to use the Port Break command.

Table 3.3: Access Rights (Continued)

Access Right	Description
P	The Port access right gives a user access to one or more serial ports and the attached serial devices. You may grant Port access rights to specific ports (Pn), a range of ports (Px-y) or all ports (PALL).

Access levels

When you specify a user's access rights, you may either specify the individual rights or you may use a shortcut that specifies an access level. The APPLIANCEADMIN and ADMIN levels are equivalent to the following individual specifications:

- The APPLIANCEADMIN level is equivalent to PALL, USER, SCON, SMON, PCON and BREAK
- The ADMIN level is equivalent to PALL, USER, SMON, PCON and BREAK

DSView software users also have access levels. Those with administrator level rights are given all CPS access rights: PCON, SCON, SMON, USER, BREAK and PALL. DSView software users with user level rights may access the serial device to which they are connected. They also have BREAK access for the port they are accessing. See the DSView Installer/User Guide for more information.

To manage a user's access rights/levels:

1. To configure a user's access rights/level, issue a User Add command, using the Access parameter to specify the rights or a level.

   USER ADD <*username*> ACCESS=<*access*>

2. To change a user's access rights/level, issue a User Set command, using the Access parameter to specify the rights or a level.

   USER SET <*username*> ACCESS=<*access*>

3. To display the access rights and level for one or all users, issue a Show User command.

   SHOW USER <*username*>|ALL

For more information, see *Managing User Accounts* on page 22 plus *User Add command* on page 70, *User Set command* on page 72 and *Show User command* on page 67.

Using Authentication Methods

The CPS appliance supports four methods for authenticating users: DS, RADIUS, local and none. Multiple connection and authentication methods may operate concurrently. By default, authentication is performed at the local CPS user database, then through the DSView software.

DS authentication

DS authentication uses one or more DSView software servers. When you specify DS authentication, you may also indicate the mode by specifying either Secure or Trustall.

- Secure indicates authentication will be locked to one DSView software server after a successful initial access, and DSView software server and appliance credentials will be stored on the CPS appliance.
- Trustall indicates that any DSView software server may be used for authentication, and DSView software server credentials will not be stored or validated on the CPS appliance.

When the secure mode is used, you may clear the stored credentials used by the DSView software at any time.

For more information, see the DSView Installer/User Guide.

Local authentication

Local authentication uses the CPS appliance internal user database to authenticate users.

RADIUS authentication

RADIUS authentication uses an external third party RADIUS server containing a user database to authenticate CPS network appliance users. The CPS appliance, functioning as a RADIUS client, sends usernames and passwords to the RADIUS server. If a username and password do not agree with equivalent information on the RADIUS server, the CPS appliance is informed and the user is denied CPS access. If the username and password are successfully validated on the RADIUS server, the RADIUS server returns an attribute that indicates the access rights defined for that username.

To use RADIUS authentication, you must specify information about the primary RADIUS server and optionally, a secondary RADIUS server to be used as a backup.

The RADIUS server definition values specified in CPS appliance commands must match corresponding values configured on the RADIUS server. On the RADIUS server, you must include CPS appliance-specific information: the list of valid users, their access rights for the CPS appliance and their preemption levels. Each user-rights attribute in the RADIUS server's dictionary must be specified as a string containing the user's access rights/level for the CPS appliance, exactly matching the syntax used in the CPS User Add command. The access rights should be followed by a space, the Preempt keyword and preemption value.

Consult your RADIUS administrator's manual for information about specifying users and their attributes. The exact process depends on the RADIUS server you are using.

No authentication

When authentication is disabled, users are not authenticated. Telnet sessions to serial ports are accepted immediately, and users are not prompted for a username or password. In this case, users are granted access only to the port to which they are connected, including Break access.

Connections to the Telnet port (23), serial CLI and PPP are still authenticated using the local CPS user database, even when authentication is expressly disabled. Generally, these communications paths are used only by administrators, and authentication is enforced in order to establish appropriate access rights.

This method cannot be used when SSH connections are enabled, nor can it be combined with any other authentication method.

Authentication of serial CLI port sessions

Using the Server CLI command, you may enable or disable user authentication at the serial CLI port. You may also configure a preemption level that will be used by a serial CLI port user when user authentication is disabled on that port. By default, authentication is enabled on the serial CLI port.

- When enabled, a serial CLI port user is authenticated against the local CPS user database, using the access rights/level and preemption level configured for that user with the User Add/User Set command.
- When disabled, a serial CLI port user is not authenticated and will be assigned the appliance administrator access level. If that CLI port user attempts to connect to another CPS port (assuming connection ability is enabled), and that port is already in use, the preemption level configured with the Server CLI command is used. For more information, see *Preemption* on page 21.

PPP sessions are always authenticated using the method specified with the Server Security command. In other words, enabling/disabling user authentication at the serial CLI port does not apply to PPP dial-in connections.

Authentication summary

The CPS appliance allows concurrent use of multiple authentication methods. This allows Telnet, SSH and DSView software clients to all access a single CPS appliance as long as the appropriate authentication methods are enabled.

For example, if you enable local and DS authentication (which is the default), DSView software clients will always be authenticated using DSView software servers. Telnet and SSH clients will be authenticated using the CPS local user database first, and DSView software second.

Similarly, if you enable DS and RADIUS authentication, DSView software clients will always be authenticated using DSView software servers. Telnet and SSH clients will be authenticated using the RADIUS servers.

As indicated above, DSView software servers will always be used for DSView software clients. For Telnet and SSH clients, the order in which you specify the authentication methods determines the order in which each method is used.

For example, if you enable local and RADIUS authentication (in that order), authentication uses the CPS user database. If that fails, authentication goes to the defined RADIUS servers. If you enable RADIUS and local authentication (in that order), authentication goes first to the defined RADIUS servers. If that fails, the local CPS user database is used.

To specify the authentication method:

1. For RADIUS authentication, issue a Server RADIUS command.

   SERVER RADIUS PRIMARY|SECONDARY IP=<*radius_ip*> SECRET=<*secret*> USER-RIGHTS=<*attr*> [AUTHPORT=<*udp*>] [TIMEOUT=<*time-out*>] [RETRIES=<*retry*>]

You must specify the server's IP address, the UDP port to be used and a "secret" to be used. You must also specify a user-rights attribute value that matches a value in the RADIUS server's dictionary.

You may also use this command to delete a RADIUS server definition.

SERVER RADIUS PRIMARY|SECONDARY DELETE

For more information, see *Server RADIUS command* on page 55.

2. Issue a Server Security command, using the Authentication parameter to specify the authentication method. Use the Encrypt parameter to enable plain text Telnet connections, SSH connections or both.

   SERVER SECURITY AUTHENTICATION=<*auth*> ENCRYPT=<*conns*>

   When SSH session access is enabled, you must specify an authentication method other than None.

3. You are prompted to save the information. Enter **Y** to confirm or **N** to cancel.

To enable or disable authentication of serial CLI port sessions:

Issue a Server CLI command, using the Auth parameter to enable/disable serial CLI port authentication and the Preempt parameter to specify the preemption level.

To clear stored DSView software authentication credentials:

Issue a Server Security command, using the DSClear parameter. This clears any stored credentials used by the DSView software.

To display authentication configuration information:

1. Issue a Show Server Security command.

   SHOW SERVER SECURITY

   The display includes the current CPS appliance authentication settings that were configured with the Server Security command. If SSH access has been enabled, the display indicates SSH2. Regardless of whether SSH is enabled, the display includes the authentication method specified with the Server SSH command.

2. To display CPS RADIUS settings that were configured with the Server RADIUS command, issue a Show Server RADIUS command.

   SHOW SERVER RADIUS

For more information, see *Server Security command* on page 57, *Show Server Security command* on page 66, *Show Server RADIUS command* on page 66 and *Connecting to devices using SSH* on page 16.

Using security lock-out

When the security lock-out feature is enabled, a user will be locked-out after five consecutive authentication failures. A successful authentication will reset the counter to zero. You may

configure a lock-out period of from 1-99 hours. Specifying a lock-out period of 0 disables the feature; that is, users will not be locked-out.

A locked-out user will remain locked-out until the specified time elapses, the CPS appliance is power-cycled or the user is unlocked by an administrator with the User Unlock command. A user with the ADMIN access level may unlock all users except a user with the APPLIANCEADMIN level. A user with the APPLIANCEADMIN level may unlock all users.

To enable or disable security lock-out:

1. To enable security lock-out, issue a Server Security command, using the Lockout parameter with a value between 1-99.
2. To disable security lock-out, issue a Server Security command, using the Lockout=0 parameter.

To unlock a locked-out user:

Issue a User Unlock command with the username.

Managing the Port History Buffer

Each CPS appliance serial port has a circular history buffer that contains the latest 64K bytes of data received from the attached serial device. This information may be helpful in analyzing attached device anomalies.

The history buffer begins filling with received data upon completion of CPS appliance initialization, even if no user is connected. When you connect to a serial port, the data that was received from the attached serial device prior to the connection is available in the buffer. Once online, new data continues to be stored in the buffer. You may choose whether to display the history buffer's content automatically when you connect and whether to keep or discard the history buffer's content at the end of a session.

When more than 64K bytes of data are sent to the history buffer, data at the top of the buffer is discarded to make room for the new data. As a result, the buffer always contains the most recent 64K bytes of port history.

Using port history mode commands

Once you are in port history mode, you may issue the commands listed in Table 3.4. Only the first letter of the command is required.

Table 3.4: Port History Mode Commands

Command	Description
Bottom	**B** sets the view location to the bottom of the file minus 23 history display lines, if available.
Clear	**C** clears the port history buffer.
Next	**N** increments the current history display line by the number of lines per page and outputs a new history display page.

Table 3.4: Port History Mode Commands (Continued)

Command	Description
Prev	**P** decrements the current history display line by the number of lines per page and outputs a new history display page.
Quit	**Q** returns to the normal CLI.
Resume	**R** leaves port history mode and CLI mode and resumes the session with the attached serial device. This single command is equivalent to sequentially using the Quit and Resume commands.
Search	**S** searches the port history buffer for a specified text string. Search strings with embedded spaces must be enclosed in quotes. By default, the search is case sensitive. To ignore case, enter **-i** before the string. To specify direction, type **-u** to search up from the current line toward the top of the buffer or **-d** to search down from the current line toward the bottom of the buffer. The search direction remains in effect for subsequent searches until you change the search direction. If the string is found, the current history display line is set to the line containing the string, and the unit outputs a history display page. If the string is not found, an error message is displayed, no other information is output and the current history display line is not changed. Entering the Search command with no parameters searches again for the previous string in the same direction as the previous search.
Top	**T** sets the current history display line to one and outputs a history display page.

The following examples assume the user is in port history mode.

The following command searches the history buffer in the upward direction for the string Abort Process.

```
PORT HISTORY> s -u "Abort Process"
```

The following command searches the history buffer for the string Process, ignoring case.

```
PORT HISTORY> s -i Process
```

For more information, see *Server CLI command* on page 51 and *Port History command* on page 46.

To access port history mode:

Issue a Port History command.

PORT HISTORY

The PORT HISTORY > prompt appears.

To control the port history buffer display when you connect:

Issue a Server CLI command, using the History parameter to specify the Hold or Auto option:

```
SERVER CLI HISTORY=HOLD|AUTO
```

- If Hold is specified, the number of bytes in the history buffer is displayed, but none of the history data is output. In this case, you must access the CLI and use the Port History command to view the port's history buffer content. This is the default mode.

- If Auto is specified, the number of bytes in the history buffer is displayed and the entire content of the buffer is output to the Telnet session. In this mode, the history buffer's content may be reviewed in the Telnet client's scrolling window. You may also use the Port History command to view the port's history buffer content.

To control the port history buffer content when you end a session:

Issue a Server CLI command, using the History parameter to specify the Clear or Keep option:

SERVER CLI HISTORY=CLEAR|KEEP

- If Clear is specified, the port history buffer is cleared and all data is discarded at the end of a session.
- If Keep is specified, the port history buffer's content is retained at the end of a session.

To clear and discard all data in a port history buffer:

Issue a Clear command while you are in port history mode.

CLEAR

- or -

Issue a Server CLI command, indicating History=Clear.

SERVER CLI HISTORY=CLEAR

In this case, the port's history buffer is cleared at the end of each device session.

Managing the CPS Appliance Using SNMP

The CPS serial over IP network appliance provides a set of commands that create and manage SNMP structures for use by third party network management products. These commands cover the following operations:

- Enabling and disabling SNMP UDP port 161 SNMP processing
- Defining read, write and trap community names
- Defining and deleting up to four SNMP management entity IP addresses
- Enabling and disabling SNMP traps
- Defining and deleting up to four trap destination IP addresses
- Defining, copying and deleting up to ten alert strings for each port

By default, SNMP is enabled but no traps are enabled and no trap destinations are defined.

To enable or disable SNMP processing:

1. To enable SNMP processing, issue a Server SNMP command with the Enable parameter. This is the default setting.

   SERVER SNMP ENABLE

2. To disable SNMP processing, issue a Server SNMP command with the Disable parameter.

   SERVER SNMP DISABLE

For more information, see *Server SNMP command* on page 58.

To specify SNMP community names:

Issue a Server SNMP Community command, using the Readcomm, Writecomm and Trapcomm parameters to specify community names.

NOTE: The default community names are “public”; if you enable SNMP, you are encouraged to change the community values to prevent access to the MIB.

SERVER SNMP COMMUNITY READCOMM=<*name*> WRITECOMM=<*name*> TRAPCOMM=<*name*>

Although all three community names default to public, if you specify a trap community name with this command, it must be different from the read and write community names.

For more information, see *Server SNMP Community command* on page 58.

To add or delete SNMP management entity addresses:

1. To add an SNMP management entity address, issue a Server SNMP Manager command with the Add parameter and the management entity’s IP address. You may define up to four SNMP management entity addresses, using separate commands.

   SERVER SNMP MANAGER ADD <*ip_address*>

   When you define at least one SNMP manager, SNMP requests are processed if they are from one of the defined SNMP managers. If a request is not from one of the defined SNMP managers, the SNMP request is discarded.
2. To delete an SNMP management entity address, issue a Server SNMP Manager command with the Delete parameter and the management entity’s IP address.

   SERVER SNMP MANAGER DELETE <*ip_address*>

If no management entities are defined, any SNMP manager may access the MIB. For more information, see *Server SNMP Manager command* on page 59.

To enable or disable SNMP traps:

1. To enable SNMP traps, issue a Server SNMP Trap command with the Enable parameter.

   SERVER SNMP TRAP ENABLE

   The CPS appliance will display a numbered list of traps that are currently disabled with a prompt requesting you to select trap(s) to enable. Indicate the traps to be enabled by entering a trap’s list number, several numbers separated by commas, a range of numbers separated by a dash or a combination of numbers with commas and dashes. To enable all traps, type **ALL**. To cancel the command, press **Enter**.

   - or -

   To enable all SNMP traps, issue a Server SNMP Trap command with the Enable and All parameters. In this case, the numbered list is not displayed.

   SERVER SNMP TRAP ENABLE ALL

2. To disable SNMP traps, issue a Server SNMP Trap command with the Disable parameter.

   SERVER SNMP TRAP DISABLE

   The CPS appliance will display a numbered list of traps that are currently enabled with a prompt requesting you to select trap(s) to disable. Indicate the traps to be disabled by entering a trap's list number, several numbers separated by commas, a range of numbers separated by a dash or a combination of numbers with commas and dashes. To disable all traps, type **ALL**. To cancel the command, press **Enter**.

   - or -

   To disable all SNMP traps, issue a Server SNMP Trap command with the Disable and All parameters. In this case, the numbered list is not displayed.

   SERVER SNMP TRAP DISABLE ALL

For more information, see *Server SNMP Trap command* on page 59 and *Supported Traps* on page 82.

To add or delete SNMP trap destination addresses:

1. To add an SNMP trap destination address, issue a Server SNMP Trap Destination command with the Add parameter and the destination's IP address. You may define up to four destination addresses, using separate commands.

   SERVER SNMP TRAP DESTINATION ADD <*ip_address*>

2. To delete an SNMP trap destination address, issue a Server SNMP Trap Destination command with the Delete parameter and the destination's IP address.

   SERVER SNMP TRAP DESTINATION DELETE <*ip_address*>

For more information, see *Server SNMP Trap Destination command* on page 60.

To add, copy or delete port alert strings:

1. To add a port alert string, issue a Port Alert Add command, specifying the port number and a 3-32 character string. You may define up to ten strings for each port, using separate commands.

   The alert string will only generate a trap if the PortAlert trap is enabled with a Server SNMP Trap command.

   PORT <*port*> ALERT ADD "<*string*>"

2. To delete a port alert string, issue a Port Alert Delete command, specifying a port number.

   PORT <*port*> ALERT DELETE

   The CPS appliance displays a numbered list of alert strings that have been defined for the specified port with a prompt requesting you to select alert string(s) to delete. Indicate the alert strings to be deleted by entering an alert string's list number, several numbers separated by commas, a range of numbers separated by a dash or a combination of numbers with commas and dashes. To delete all alert strings, type **ALL**. To cancel the command, press **Enter**.

3. To copy the defined alert strings from one port to another port, issue a Port Alert Copy command, specifying the port numbers to be copied to and from.

PORT <*to_port*> ALERT COPY <*from_port*>

At the confirmation prompt, press **Y** to confirm or **N** to cancel. When the copy operation occurs, all previously defined strings on the port being copied to will be replaced.

For more information, see *Port Alert Add command* on page 45, *Port Alert Copy command* on page 45 and *Port Alert Delete command* on page 46.

To display SNMP configuration information:

Issue a Show Server SNMP command.

SHOW SERVER SNMP

The display includes information specified with the Server SNMP, Server SNMP Community, Server SNMP Manager, Server SNMP Trap and Server SNMP Trap Destination commands.

For more information, see *Show Server SNMP command* on page 67.

To display port alert string information:

Issue a Show Port Alert command, specifying a port number.

SHOW PORT <*port*> ALERT

The display lists all the port's defined alert strings.

For more information, see *Show Port Alert command* on page 64.

CHAPTER 4

Using CPS Appliance Commands

Accessing the CLI

You may access the CLI in three ways: using the Telnet CLI, using the serial CLI or entering the CLI access character during a session to a serial device. When the CLI is accessed, its prompt appears (>), indicating you may type a command.

Entering Commands

At the command prompt, type a command and then press **Return** or **Enter**. When the key is pressed, the command line comprises all characters to the left of the cursor. The character at the cursor and any characters to the right of the cursor are ignored. Table 4.1 lists the line editing operations for VT100 compatible devices.

Table 4.1: Line Editing Operations for VT100 Compatible Devices

Operation	Action
Backspace	The character immediately before the cursor is erased and all text at and to the right of the cursor moves one character to the left.
Left Arrow	If the cursor is not at the beginning of the line, the cursor moves one character to the left. If the cursor is at the beginning of the line, no action is taken.
Right Arrow	If the cursor is not at the end of the line, the cursor moves one character to the right. If the cursor is at the end of the line, no action is taken.
Up Arrow	The CLI maintains a buffer containing the last 16 typed command lines. If there is a previous command line, it will be output as the current command line and may be edited. If there is no previous command line in the command line buffer, the command line is set to blanks and you may enter a new command.
Down Arrow	The next command in the CLI command line buffer is made available for edit. If there is no next command line, the command line is set to blanks and you may enter a new command.
Delete	The character at the cursor position is deleted and all characters to the right of the cursor position are moved left one character.

Table 4.2 lists the line editing operations for ASCII TTY devices. There is no command line buffer available on an ASCII TTY device.

Table 4.2: Line Editing Operations for ASCII TTY Devices

Operation	Action
Backspace	Erases the last character typed.
Esc	Erases the current command line.

When commands take effect

Each command is completely processed before the next command may be entered. Some commands prompt for confirmation before they are processed. In these cases, you must confirm or cancel by entering **Y** or **N** respectively.

If you enter a Server FLASH command or if you change the CPS appliance IP address with a Server Set command, a reboot is required before the change becomes effective. In these cases, the CPS database is updated when you enter the command and you are prompted that the change will not take effect until the CPS appliance reboots. You may choose to reboot at that time, or you may decline. When the unit reboots, your session and all other sessions on the CPS appliance are terminated.

Understanding Conventions

This section describes the parts of a CPS appliance command and the conventions used in this document to describe a command's syntax.

Command syntax

A command may have four types of syntax: positional commands, positional parameters, keyword parameters and keyword values. The following examples demonstrate the syntax types.

The following Set Port command changes the baud rate and flow control settings for port 2.

```
> PORT 2 SET BAUD=57600 FLOW=XONXOF
```

Table 4.3: Command Syntax Types in Example Command

Value	Syntax
PORT	Positional command.
2	Positional parameter that indicates the port number for the command.
SET	Positional command that indicates port settings are to be changed.
BAUD	Keyword parameter, which is always followed by an equal (=) sign.
57600	Keyword value indicating the baud rate value for the BAUD keyword parameter.
FLOW	Keyword parameter, which is always followed by an equal (=) sign.

Table 4.3: Command Syntax Types in Example Command (Continued)

Value	Syntax
XONXOF	Keyword value.

Not every command will contain all syntax types. For example, the following command reboots the CPS appliance.

```
>SERVER REBOOT
```

In this case, both SERVER and REBOOT are positional commands.

In most cases, one or more spaces separate positional commands, positional parameters and keyword parameters.

For most positional commands, positional parameters or keyword parameters, you only need to enter the first three characters. The exceptions are:

- When you specify a terminal type with the Type parameter in the Server CLI command, you must enter all characters.
- When you specify an authentication method with the Auth parameter in the Server SSH command, you must enter all characters.
- When you specify control signal monitoring with the Power parameter in the Port Set command, you must enter all characters.

With the exception of usernames and passwords, commands are not case sensitive; they may be entered in uppercase, lowercase or a combination. For example, all of the following commands are correct.

```
> PORT 2 SET BAUD=57600 FLOW=XON
> POR 2 SET BAU=57600 FLOW=XON
> por 2 Set Baud=57600 flow=xon
> port 2 set baud=57600 flow=xon
```

NOTE: Usernames and passwords are case sensitive. These values are stored exactly as you enter them. For example, the username “Ann” must be entered with an uppercase “A” and all other letters lowercase. The username “ANN” will not be accepted as the username “Ann.” Usernames and passwords must contain 3-16 alphanumeric characters.

Any syntax errors are displayed, and where applicable, the error is underlined.

In the following example, the keyword parameter “baud” is misspelled. Even if more than three characters are entered, they must all be correct.

```
> port 2 Set Baux=57600 flow=xon
           ----
ERR 26 - SET keyword parameter invalid
```

In the following example, the keyword value “576” is not valid. Numeric keyword values must be fully specified and may not be shortened to three characters.

```
> POR 2 SET BAUD=576 FLOW=XON
                    ---
ERR 27 - SET keyword value invalid
```

In the following example, there are spaces between BAUD, the equal sign and the value 57600. Spaces are not permitted between keyword parameters and their values.

```
> POR 2 SET BAUD = 57600 FLOW=XON
              ------------
ERR 26 - SET keyword parameter invalid
```

Syntax conventions

This manual uses the following command syntax conventions:

- Brackets [ ] surround optional keywords and values.
- Angle brackets < > surround user-supplied positional parameters and keyword parameter values.
- In most cases, choices are separated by a vertical bar |. The description indicates if you may specify more than one of the choices and how to separate multiple values. The exception is the Server SSH command. In this case, the vertical bar is specified on the command line when you wish to enable the “password or key” method (PW|KEY) or the “key or password” method (KEY|PW).

Command Summary

Table 4.4 lists the CPS appliance commands, including a brief description plus the required access rights and level.

Table 4.4: CPS Appliance Command Summary

Command	Description, Access Right and Access Level
Connect	Accesses devices from the serial CLI port. Access right: port-specific Access level: ADMIN or APPLIANCEADMIN (Users who do not have the ADMIN or APPLIANCEADMIN level must have the appropriate port access configured to issue this command.)
Disconnect	Ends a device session initiated with Connect command. Access right: port-specific Access level: ADMIN or APPLIANCEADMIN (Users who do not have the ADMIN or APPLIANCEADMIN level must have the appropriate port access configured to issue this command.)
Help	Displays information about commands. Access right: none needed Access level: all
Port Alert Add	Adds a port alert string. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN

Table 4.4: CPS Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
Port Alert Copy	Copies a port's alert strings to another port. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Port Alert Delete	Deletes one or more port alert strings. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Port Break	Sends a break signal to the attached device. Access right: BREAK Access level: ADMIN or APPLIANCEADMIN
Port History	Accesses the port history buffer. Access right: none needed Access level: all
Port Logout	Terminates the CPS session on a specified port. Access right: USER Access level: ADMIN or APPLIANCEADMIN
Port Set	Changes port settings. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
Quit	Terminates the current CPS session. Access right: none needed Access level: all
Resume	Resumes device connection after being in CLI mode. Access right: none needed Access level: all
Server CLI	Specifies the serial CLI port, port type and access character; enables/disables device connection from the CLI port and authentication of CLI port sessions; specifies a modem initialization string; specifies port history mode operations and a port time-out value. Access right: SCON Access level: APPLIANCEADMIN
Server FLASH	Updates the unit's FLASH. Access right: SCON Access level: APPLIANCEADMIN
Server Ping	Enables/disables response to ping requests. Access right: SCON Access level: APPLIANCEADMIN
Server PPP	Enables/disables a PPP server on the serial CLI port. Access right: SCON Access level: APPLIANCEADMIN

Table 4.4: CPS Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
Server RADIUS	Specifies RADIUS server parameters. Access right: SCON Access level: APPLIANCEADMIN
Server Reboot	Reboots the unit. Access right: SCON Access level: APPLIANCEADMIN
Server Security	Specifies the user authentication mode, enables/disables security lock-out and connection methods. Access right: SCON Access level: APPLIANCEADMIN
Server Set	Changes the CPS appliance network configuration. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP	Enables/disables UDP port 161 SNMP processing. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP Community	Defines read, write and trap SNMP community strings. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP Manager	Defines/deletes SNMP management entities. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP Trap	Enables/disables SNMP traps. Access right: SCON Access level: APPLIANCEADMIN
Server SNMP Trap Destination	Defines/deletes destinations for enabled SNMP traps. Access right: SCON Access level: APPLIANCEADMIN
Server SSH	Enables/disables SSH session access to the CPS appliance and specifies the SSH authentication method. Access right: SCON Access level: APPLIANCEADMIN
Show Port	Displays port configuration information and statistics. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Port Alert	Displays a port's alert strings. Access right: SMON Access level: ADMIN or APPLIANCEADMIN

Table 4.4: CPS Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
Show Server	Displays CPS appliance configuration, statistics and session information. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server CLI	Displays information specified with the Server CLI command. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server PPP	Displays PPP settings. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server RADIUS	Displays RADIUS settings. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server Security	Displays authentication and lock-out settings. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show Server SNMP	Displays SNMP configuration information. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
Show User	Displays user configuration and session information. Access right: SMON Access level: ADMIN or APPLIANCEADMIN
SPC	Changes SPC port settings. Access right: SCON or PCON Access level: ADMIN or APPLIANCEADMIN
User Add	Adds a new user. Access right: USER Access level: ADMIN or APPLIANCEADMIN
User Delete	Deletes a user. Access right: USER Access level: ADMIN or APPLIANCEADMIN
User Logout	Terminates a user's session. Access right: USER Access level: ADMIN OR APPLIANCEADMIN (An ADMIN level user may issue this command for users with any level other than APPLIANCEADMIN.)
User Set	Changes a user's configuration information. Access right: USER Access level: ADMIN or APPLIANCEADMIN

Table 4.4: CPS Appliance Command Summary (Continued)

Command	Description, Access Right and Access Level
User Unlock	Unlocks a locked-out user. Access right: USER Access level: ADMIN or APPLIANCEADMIN (An ADMIN level user may issue this command for users with any level other than APPLIANCEADMIN.)

CHAPTER 5

CPS Appliance Commands

Connect Command

The Connect command establishes a connection from the CPS serial over IP network appliance serial CLI port to a device attached to another port on that CPS appliance. To use this command, you must have previously issued a Server CLI command with the Connect=On parameter. For more information, see *Connecting to Serial Devices* on page 13.

Access right: port-specific
Access level: ADMIN, APPLIANCEADMIN or others with access to port

Syntax

CONNECT <*port*>

Table 5.1: Connect Command Parameter

Parameter	Description
<*port*>	Port number in the range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance.

Example

The following command establishes a connection from the serial CLI port to port 6.

```
> connect 6
```

Disconnect Command

The Disconnect command terminates a session with a serial device that was previously initiated with a Connect command. This command frees the attached serial device and allows other users to access it.

Access right: port-specific
Access level: ADMIN, APPLIANCEADMIN or others with access to port

Syntax

DISCONNECT

Help Command

The Help command displays information about CPS appliance commands.

Access right: none needed
Access level: none needed

Syntax

HELP [<*command_name*>]

Table 5.2: Help Command Parameter

Parameter	Description
<*command_name*>	Command name. Default: Displays list of all commands

Examples

The following command displays information about the Show Server CLI command.

```
help sho ser cli
```

The following command displays a list of all commands.

```
help
```

Port Commands

The Port command has several forms, as listed in Table 5.3.

Table 5.3: Port Command Summary

Command	Description
Port Alert Add	Adds a port alert string to a specified port.
Port Alert Copy	Copies port alert strings from one port to another port.
Port Alert Delete	Deletes one or more port alert strings from a specified port.
Port Break	Sends a serial break signal to the attached device.
Port History	Accesses a port's history mode.
Port Logout	Terminates the CPS session on a specified port.
Port Set	Changes CPS serial port settings for one or all ports.
Port Set In/Out	Specifies how carriage returns and linefeeds are treated in incoming or outgoing serial data.

Port Alert Add command

The Port Alert Add command adds a port alert string to a specified port. Each port may have up to ten port alert strings. Duplicate strings are not allowed on the same port. To generate a trap, the Server SNMP Trap command must be issued to enable the PortAlert trap. For more information, see *Managing the CPS Appliance Using SNMP* on page 30.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*port*> ALERT ADD "<*string*>"

Table 5.4: Port Alert Add Command Parameters

Parameter	Description
<*port*>	Port number in the range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance.
<*string*>	3-32 character string. If the string contains embedded spaces, it must be enclosed in quotes.

Port Alert Copy command

The Port Alert Copy command copies the alert strings from one port (from_port) to another (to_port). Any alert strings that were previously defined on the to_port will be deleted. When you enter this command, you are prompted to confirm or cancel the copy operation.

For more information, see *Managing the CPS Appliance Using SNMP* on page 30.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*to_port*> ALERT COPY <*from_port*>

Table 5.5: Port Alert Copy Command Parameters

Parameter	Description
<*to_port*>	Port number where alert strings will be copied, in the range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance.
<*from_port*>	Port number from which alert strings will be copied, in the range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance.

Example

The following command copies the alert strings defined on port 1 to port 7, replacing any previously defined alert strings on port 7.

```
port 7 alert copy 1
```

Port Alert Delete command

The Port Alert Delete command deletes one or more alert strings from a port. When you issue this command, a numbered list of defined alert strings is displayed, from which you choose those to be deleted. You may enter one or more numbers separated by commas, a range of numbers separated by a hyphen or type **ALL** to specify all strings. Pressing **Enter** cancels the command.

For more information, see *Managing the CPS Appliance Using SNMP* on page 30.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*port*> ALERT DELETE

Table 5.6: Port Alert Delete Command Parameter

Parameter	Description
<*port*>	Port number in the range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance.

Example

The following command deletes defined alert strings from port 3.

```
> PORT 3 ALERT DELETE
Alert-strings assigned to port 3:
1) The first alert string
2) The second alert string
3) The third alert string
4) The fourth alert string
Select Alert-string(s) to delete>
```

The alert string numbers specified at the prompt will be deleted.

Port Break command

The Port Break command sends a serial break signal to the device to which you are attached.

Access right: BREAK
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT BREAK

Port History command

The Port History command accesses a serial port's history mode while you are attached to the port. When you are in history mode, the PORT HISTORY> prompt appears, and you may search the port's history buffer for specified strings.

For more information, see *Managing the Port History Buffer* on page 28.

Access right: none needed
Access level: all

Syntax

PORT HISTORY

When you are in port history mode, you may issue the commands listed in Table 3.4 on page 28.

Examples

The following command accesses the serial port's history mode.

```
> port history
```

In history mode, the following command searches the history buffer in the downward direction for the string "connected to," ignoring case.

```
PORT HISTORY > s -d -i "connected to"
```

Port Logout command

The Port Logout command terminates the CPS appliance session on a specified port.

Access right: USER
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT <*port*> LOGOUT

Table 5.7: Port Logout Command Parameter

Parameter	Description
<*port*>	Port number in the range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance.

Port Set command

The Port Set command changes serial port settings in the CPS configuration database. At least one keyword parameter and value must be specified. Some changes become effective upon the next connection to the port.

For more information, see *Configuring Serial Port Settings* on page 11.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT [<*port*>|ALL] SET
[TD=<*device*>] [NAME=<*name*>] [BAUD=<*baud*>] [SIZE=<*size*>] [PARITY=<*parity*>]

[STOP=<*stopbits*>] [FLOW=<*signal*>] [TIMEOUT=<*time-out*>] [SOCKET=<*socket*>] [CHAR=^<*cli_char*>] [TOGGLE=NONE|DTR] [POWER=<*signal*>]

Table 5.8: Port Set Command Parameters

Parameter	Description
<*port*>|ALL	A port number in range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance, a range of ports separated by a hyphen or multiple port numbers separated by commas, or All which indicates that the settings that follow should be applied to all ports. Default = port to which you are attached
TD=<*device*>	Target device type. Valid values are Console and SPC. If SPC is specified, no other port configuration values may be changed with this command. Default = Console
NAME=<*name*>	Port name, up to 32 characters. If the name contains spaces, enclose the name in double quotes. To return one or all port names to default values, specify Name="". Default = last 3 octets of MAC address plus the port number
BAUD=<*baud*>	Baud rate. Valid values are: 0, 75, 110, 134, 150, 200. 300, 600, 1200, 2400, 4800, 7200, 9600, 14400, 19200, 28800, 38400, 57600, 115200. Default: = 9600
SIZE=<*size*>	Number of data bits per character. Valid values are 7 and 8. Default = 8
PARITY=<*parity*>	Parity. Valid values are: None No parity. Even Even parity. Odd Odd parity. Mark Mark parity. Space Space parity. Default = None
STOP=<*stopbits*>	Number of stop bits per character. Valid values are 1 and 2. Default = 1
FLOW=<*signal*>	Flow control signal. For hardware flow control, be sure the control signals are correctly wired, or data loss may occur. The flow control signal cannot also be used for power status monitoring. Valid values are: XONXOF Software XON/XOFF flow control. RTSCTS Hardware RTS/CTS flow control. DTRDCD Hardware DTR/DCD flow control. None No flow control. Default = None
TIMEOUT=<*time-out*>	Number of time-out minutes in the range 0-90. If no data is received or transmitted during a Telnet session for the specified period, the session will time-out. A zero value indicates no time-out. This value overrides the time-out value set with a Server CLI command. Default = use value set with Server CLI command

Table 5.8: Port Set Command Parameters (Continued)

Parameter	Description
SOCKET=<*socket*>	TCP port that must be entered on the Telnet client to connect to this serial port. The new value becomes effective in subsequent sessions. When SSH is enabled, the CPS appliance automatically adds 100 to the specified value. When All is specified, port 1 will be assigned the specified socket value plus 1, port 2 will be assigned the specified value plus 2, and so on. When All is specified and SSH is enabled, port 1 will be assigned the specified socket value plus 101, port 2 will be assigned the specified value plus 102, and so on. Default = 3000 plus the port number, 3100 plus the port number if SSH is enabled; see above for action taken if All is specified
CHAR=^<*cli_char*>	CLI access character in the range A to _ (underscore) or None. (The allowable ASCII range is 0x41-0x5F and 0x61-0x7A.) The CLI access character, when pressed simultaneously with the **Ctrl** key during a session with an attached serial device, will suspend the session with the device and place you in CLI command mode. If None is specified, the value specified in the Char parameter of the Server CLI command will be used. Default = None
TOGGLE=NONE|DTR	When set to DTR, the CPS appliance will toggle the port's DTR-out signal off for 1/2 second each time a connection is made to the port. This toggle is required to awaken the console port of some devices. Default=None
POWER=<*signal*>	Control signal to monitor and the state that indicates the target device has power on. The entire value must be specified; abbreviations are not allowed. The power status monitoring signal cannot also be used for flow control. Valid values are: None Disables power status monitoring. HICTS CTS high indicates power on. LOCTS CTS low indicates power on. HIDCD DCD high indicates power on. LODCD DCD low indicates power on. HIDSR DSR high indicates power on. LODSR DSR low indicates power on. Default = None

Example

The following command sets a baud rate of 57600 and enables XON/XOFF flow control on port 2.

```
> port 2 set baud=57600 flow=xonxof
```

Port Set In/Out command

The Port Set In/Out command specifies how carriage returns (CR) and linefeeds (LF) are treated in incoming or outgoing serial data on one or all ports.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

PORT [<*port*>|ALL] SET IN|OUT [CR=<*cr*>] [LF=<*lf*>|CRLF=CR]

Table 5.9: Port Set In/Out Command Parameters

Parameter	Description
<*port*>|ALL	Either a port number in range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance, or All which indicates that the settings that follow should be applied to all ports. Default = port to which you are attached
ALL	Indicates that the settings that follow should be applied to all ports.
IN|OUT	Either In to specify translation for incoming data or Out to specify translation for outgoing data.
CR=<*cr*>	Translation to be made for carriage returns. Valid values are: CR=CR Carriage return is treated as a carriage return. CR=LF Carriage return is treated as a linefeed. CR=STRIP Carriage return is stripped. CR=CRLF Carriage return is treated as a carriage return and linefeed. Default: CR=CR
LF=<*lf*>|CRLF=CR	Translation to be made for linefeeds. Valid values are: LF=LF Linefeed is treated as a linefeed. LF=CR Linefeed is treated as a carriage return. LF=STRIP Linefeed is stripped. CRLF=CR Linefeed is stripped only if it is preceded by a carriage return. This LF setting cannot be specified with any other LF setting. Default: LF=LF

Quit Command

The Quit command terminates the current CPS appliance session and terminates your Telnet connection to the unit.

Access right: none needed
Access level: all

Syntax

QUIT

Resume Command

The Resume command exits the CLI and resumes your connection to the attached serial device. The history buffer contains any data received while you were in CLI mode.

Access right: none needed
Access level: all

Syntax

RESUME

Server Commands

The Server command has several forms, as listed in Table 5.10.

Table 5.10: Server Command Summary

Command	Description
Server CLI	Specifies the serial CLI port, type and access character; modem initialization string; port history mode operations and port time-out value. It also enables/disables device connection from the CLI port.
Server FLASH	Updates the unit's FLASH.
Server Ping	Enables/disables response to ping requests.
Server PPP	Enables/disables PPP connections to the serial CLI port.
Server RADIUS	Specifies RADIUS server parameters.
Server Reboot	Reboots the unit.
Server Security	Specifies user authentication method, enables/disables security lock-out and enables/disables connection methods.
Server Set	Changes the CCM appliance network configuration.
Server SNMP	Enables/disables UDP port 161 SNMP processing.
Server SNMP Community	Defines read, write and trap SNMP community strings.
Server SNMP Manager	Defines/deletes SNMP management entities.
Server SNMP Trap	Enables/disables SNMP traps.
Server SNMP Trap Destination	Defines/deletes destinations for enabled SNMP traps.
Server SSH	Enables/disables SSH session access to the CPS appliance and specifies the SSH authentication method.

Server CLI command

The Server CLI command:

- Specifies the CLI port, type and access character
- Enables or disables device connection from the CLI port
- Specifies a modem initialization string
- Specifies port history mode operations

- Specifies a port time-out value
- Enables/disables serial CLI port authentication
- Specifies a preemption level to be used for serial CLI port sessions when authentication is disabled on that port

At least one parameter must be specified.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER CLI [PORT=<*port*>] [TYPE=<*type*>] [CHAR=^<*char*>] [CONNECT=ON|OFF] [HISTORY=HOLD|AUTO,CLEAR|KEEP] [MODEMINIT="<*string*>"] [TIMEOUT=<*time-out*>] [AUTH=ENABLE|DISABLE] [PREEMPT=1|2|3|4]

Table 5.11: Server CLI Command Parameters

Parameter	Description
PORT=<*port*>	CLI port number in the range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance. Default = 1
TYPE=<*type*>	Terminal type to be used on the CLI port. The entire name of the type must be specified; abbreviations are not permitted. Valid types are: ASCII, VT52, VT100, VT102, VT220, VT320 and OFF. Specifying Type=Off disables the CLI. Default: ASCII
CHAR=^<*char*>	CLI access character in the range A through _ (underscore). (The allowable ASCII range is 0x41-0x5F and 0x61-0x7A.) The CLI access character, when pressed simultaneously with the **Ctrl** key during a session with an attached serial device, will suspend the session with the device and place you in CLI command mode. This value will be used if a port's Port Set command contains a Char=None parameter. Default = ^d
CONNECT=ON|OFF	Enables or disables the ability to use the Connect command from the serial CLI port. When enabled, a serial CLI user may use the Connect command to establish a connection to the serial device attached to another CPS appliance serial port. When disabled, you cannot use the Connect command from the serial CLI port. Default = ON
HISTORY=HOLD|AUTO, CLEAR|KEEP	Port history file processing options during connection (Hold or Auto) and when a session ends (Clear or Keep): Hold — Upon connection you are informed of how much data is in the history buffer, but the data is not displayed. Auto — Upon connection you are informed of how much data is in the history buffer, and it is then displayed. Clear — The history buffer's content is cleared when a session ends. Keep — The history buffer's content is retained when a session ends. You cannot specify both Clear and Keep or both Hold and Auto. Default = HOLD,CLEAR

Table 5.11: Server CLI Command Parameters (Continued)

Parameter	Description
MODEMINIT="<*string*>"	Modem initialization string, enclosed in quotation marks. Must contain at least ATV1 and S0=1. Default = "" (no modem is attached to serial CLI port)
TIMEOUT=<*time-out*>	Number of time-out minutes in the range 0-90. If no data is received or transmitted during a Telnet session for the specified period, the session will time-out. A zero value indicates no time-out. This value is used for any CPS port that does not have a time-out value set with the Port Set command, during a Telnet session to port 23 or an SSH session to port 22. Default = 15 minutes
AUTH=ENABLE|DISABLE	Enables or disables authentication of serial CLI port sessions. When enabled, serial CLI sessions are authenticated against the local user database. When disabled, serial CLI sessions are not authenticated, the user is assigned the appliance administrator level and the preemption level specified with the Preempt parameter will be used. Default = enabled
PREEMPT=1|2|3|4	Preemption level for serial CLI session users when authentication is disabled for the serial CLI port (Auth=disable). Default = 4

Server FLASH command

The Server FLASH command updates the CPS program images in FLASH memory. You may wish to use this command to update the program with new features or to install a later release of the program.

There are two program images that you may update in the CPS FLASH. The boot image file (cps10bt.img) contains the CPS startup and self-test logic. The application image (cps10app.img) contains the program that provides CPS functionality.

You will need a TFTP server. Download the latest FLASH image from Avocent. Save the image file to the appropriate directory on the TFTP server.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER FLASH BOOT|APP HOSTIP=<*tftp_add*> IMAGE=<*host_file*>

Table 5.12: Server FLASH Command Parameters

Parameter	Description
BOOT|APP	Indicates either the boot image should be updated or the application image should be updated.
HOSTIP=<*tftp_add*>	IP address of TFTP server host.

Table 5.12: Server FLASH Command Parameters (Continued)

Parameter	Description
IMAGE=<*host_file*>	Name of file on TFTP server host containing the image file.

Example

The following command updates the boot image program using the image file name c:\winnt\system32\drivers\cps10bt.img, which is located on the TFTP server host located at 192.168.1.16.

```
> ser fla app hostip=192.168.1.16
c:\winnt\system32\drivers\ima=cps10bt.img
```

Server Ping command

The Server Ping command enables or disables response to ping requests. When enabled, the CPS appliance receives and responds to all ping requests. When disabled, ping requests are received and silently discarded.

Syntax

SERVER PING [ENABLE|DISABLE]

Table 5.13: Ping Command Parameter

Parameter	Description
ENABLE|DISABLE	Enables or disables response to the ping requests. Default = Enabled

Server PPP command

The Server PPP command enables or disables the PPP server on the serial CLI port. For more information, see *Connecting to devices using PPP* on page 15.

Once the PPP server has been configured with this command by specifying the required addresses and masks, those values remain in the database. Later, if you disable the PPP server and wish to reenable it with the same addresses, you don't need to specify the address values again.

When you enable the PPP server, the serial CLI port must already be defined.

When you enter this command, you are prompted to confirm or cancel the specified changes.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER PPP DISABLE|ENABLE
LOCALIP=<*local_ip*>] [REMOTEIP=<*rem_ip*>] [MASK=<*subnet*>]

Table 5.14: Server PPP Command Parameters

Parameter	Description
DISABLE|ENABLE	Disables or enables the PPP server.
LOCALIP=<*local_ip*>	IP address to be used to connect the CPS appliance over the PPP connection. Must be on same subnet as REMOTEIP address.
REMOTEIP=<*rem_ip*>	IP address to assign to the PPP client end of the PPP connection. Must be on same subnet as LOCALIP address.
MASK=<*subnet*>	LAN subnet for the PPP dial-in client.

Examples

The following command enables the PPP server with a local IP address of 192.168.0.1, a remote IP address of 192.168.0.2 and a subnet mask of 255.255.255.0.

```
> ser ppp ena loc=192.168.0.1 rem=192.168.0.2 mas=255.255.255.0
```

The following command enables the PPP server with previously configured IP and subnet mask values. This form of the command would not be valid unless the IP and subnet mask values had been previously configured.

```
> server ppp enable
```

Server RADIUS command

The Server RADIUS command defines or deletes RADIUS parameters for the CPS RADIUS client. For more information, see *RADIUS authentication* on page 25.

When you enter this command, you are prompted to confirm or cancel the specified changes.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER RADIUS PRIMARY|SECONDARY
IP=<*radius_ip*> SECRET=<*secret*> USER-RIGHTS=<*attr*>
[AUTHPORT=<*udp*>] [TIMEOUT=<*time-out*>] [RETRIES=<*retry*>]
- or -
SERVER RADIUS PRIMARY|SECONDARY DELETE

Table 5.15: Server RADIUS Command Parameters

Parameter	Description
PRIMARY| SECONDARY	Indicates either the primary RADIUS server or the secondary RADIUS server is being defined or deleted.
IP=<*radius_ip*>	IP address of the RADIUS authentication server.
SECRET=<*secret*>	8-24 character text string for shared secret with the RADIUS server. Enclose the string in quotes if it contains spaces.
USER-RIGHTS=<*attr*>	Attribute number defined on the RADIUS server, in the range 1-255.
AUTHPORT=<*udp*>	UDP port for RADIUS authentication server, in the range 1-65535. This value is usually 1645, but may be 1812. Default = 1645
TIMEOUT=<*time-out*>	Number of seconds to wait for a response from the RADIUS server, in the range 1-60. Default = 5
RETRIES = <*retry*>	Number of attempts to make to authenticate a user after a time-out, in the range 1-10. Default = 3
DELETE	Deletes the RADIUS server definition.

Examples

The following command specifies primary RADIUS server information; default values will be used for the UDP port, time-out and retries values.

```
> ser radius primary ip=192.168.0.200 secret=ThePrimaryRadSecret user-rights=86
```

The following command deletes the primary RADIUS server definition.

```
> ser radius primary del
```

Server Reboot command

The Server Reboot command reboots the CPS appliance. During a reboot, any active Telnet sessions, including your own, are terminated, and all users are informed accordingly. Any configuration changes that require a reboot will become effective when the reboot completes.

When you enter this command, you are prompted to confirm or cancel the reboot.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER REBOOT

Server Security command

The Server Security command specifies the authentication method, enables/disables access methods and enables/disables security lock-out. For more information, see *Using Authentication Methods* on page 24, *Enabling plain text Telnet and SSH connections* on page 19 and *Using security lock-out* on page 27.

When you enter this command, you are prompted to confirm or cancel the specified information.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SECURITY [AUTHENTICATION=<*auth*>] [ENCRYPT=<*conns*>] [DSMODE=SECURE|TRUSTALL] [DSCLEAR] [LOCKOUT=<*hours*>]

Table 5.16: Server Security Command Parameters

Parameter	Description
AUTHENTICATION=<*auth*>	Authentication method. Multiple values may be specified, separated by commas. Valid values are: DS Use DSView software server(s) for authentication. LOCAL Use the local CPS user database to authenticate users. RADIUS Use the previously defined RADIUS server(s) to authenticate users. NONE Do not authenticate users. This method cannot be used when SSH access is enabled, and it cannot be combined with other authentication methods. Default = LOCAL,DS
ENCRYPT=<*conns*>	Enables/disables plain text Telnet or SSH connections. To enable both, specify both values, separated by a comma. Valid values are: SSH Enables SSH connections. None Enables plain text Telnet connections. Default = None
DSMODE=SECURE|TRUSTALL	Specifies the mode when DSView software authentication is used. Secure indicates authentication will be locked to one DSView software server after initial access, and DSView software server and appliance credentials will be stored. Trustall indicates that any DSView software server may be used for authentication, and DSView software server credentials will not be stored or validated.
DSCLEAR	Clears any stored credentials used by the DSView software, including the DSMode setting.
LOCKOUT=<*hours*>	Enables or disables security lock-out. To enable, specify the number of hours in the lock-out period, in the range 1-99. To disable, specify a zero value. Default = 0 (disabled)

Server Set command

The Server Set command changes CPS appliance address information. You may specify one, two or all three parameters. A reboot is required if you change the IP address.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SET [IP=<*ip_address*>] [MASK=<*subnet*>] [GATEWAY=<*gtwy*>]

Table 5.17: Server Set Command Parameters

Parameter	Description
IP=<*ip_address*>	IP address.
MASK=<*subnet*>	Subnet mask for the subnet on which the CPS appliance resides.
GATEWAY=<*gtwy*>	IP address of default gateway for routing IP packets.

Server SNMP command

The Server SNMP command enables or disables SNMP UDP port 161 SNMP processing. When you disable SNMP processing, you may still enable and disable traps with the Server SNMP Trap command.

For more information, see *Managing the CPS Appliance Using SNMP* on page 30.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP ENABLE|DISABLE

Table 5.18: Server SNMP Command Parameter

Parameter	Description
ENABLE|DISABLE	Enables or disables SNMP processing. Default = Enabled

Server SNMP Community command

The Server SNMP Community command defines read, write and trap SNMP community strings. Community names are case sensitive.

NOTE: The default community names are “public”; if you enable SNMP, you are encouraged to change the community values to prevent access to the MIB.

For more information, see *Managing the CPS Appliance Using SNMP* on page 30.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP COMMUNITY [READCOMM=<*name*>] [WRITECOMM=<*name*>] [TRAPCOMM=<*name*>]

Table 5.19: Server SNMP Community Command Parameters

Parameter	Description
READCOMM=<*name*>	1-64 alphanumeric character read community name. Default = public
WRITECOMM=<*name*>	1-64 alphanumeric character write community name. Default = public
TRAPCOMM=<*name*>	1-64 alphanumeric character trap community name. If you specify this parameter, the name must be different from the read and write community names. Default = public

Server SNMP Manager command

The Server SNMP Manager command defines or deletes SNMP management entities. You may define up to four management entities. If you delete all SNMP managers (or never add any), the CPS appliance may be accessed using SNMP from any IP address.

For more information, see *Managing the CPS Appliance Using SNMP* on page 30.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP MANAGER ADD|DELETE <*ip_address*>

Table 5.20: Server SNMP Manager Command Parameters

Parameter	Description
ADD|DELETE	Adds or deletes the specified SNMP management entity.
<*ip_address*>	IP address of SNMP management entity.

Example

The following command adds an SNMP management entity with the IP address of 192.168.0.1.

```
server snmp manager add 192.168.0.1
```

Server SNMP Trap command

The Server SNMP Trap command enables or disables SNMP traps. When you issue this command with the Enable parameter, the CPS appliance displays a numbered list of all currently disabled traps. When you issue this command with the Disable parameter, a numbered list of all currently enabled traps is displayed.

You may indicate the traps to be enabled/disabled by entering a single number, several numbers separated by commas, a range of numbers separated by a dash or a combinations of numbers separated by commas and dashes. You may also type **ALL** to select all traps in the list or press **Enter**, which cancels the operation.

If you specify **ALL** on the command line, the numbered list is not displayed.

If you enable a trap but there is no trap destination configured for it, a warning will be issued. In this case, issue a Server SNMP Trap Destination command.

NOTE: By default, all traps are disabled. The PortAlert trap must be enabled for port alert processing to be performed.

For more information, see *Managing the CPS Appliance Using SNMP* on page 30. See *Supported Traps* on page 82 for a list of supported traps.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP TRAP [ENABLE|DISABLE] [ALL]

Table 5.21: Server SNMP Trap Command Parameter

Parameter	Description
ENABLE|DISABLE	Enable generates a numbered list of currently disabled traps from which you choose those to enable. Disable generates a numbered list of currently enabled traps from which you choose those to disable.

Example

The following command enables the linkUp, userDeleted and userLogin SNMP traps.

```
server snmp trap enable
Traps now disabled:
1) linkUp        4) userLogin
2) userAdded     5) imageUpgradeStarted
3) userDeleted
Select trap(s) to enable>1,3-4
```

Server SNMP Trap Destination command

The Server SNMP Trap Destination command defines or deletes destinations for enabled SNMP traps. Once you define destinations for enabled SNMP traps, when a trap occurs, the CPS appliance will generate SNMP trap messages to each defined SNMP trap destination. You may define up to four trap destinations, using separate commands.

For more information, see *Managing the CPS Appliance Using SNMP* on page 30.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SNMP TRAP DESTINATION ADD|DELETE <*ip_address*>

Table 5.22: Server SNMP Trap Destination Command Parameters

Parameter	Description
ADD|DELETE	Defines or deletes the specified destination.
<*ip_address*>	IP address of trap destination.

Server SSH command

The Server SSH command enables or disables SSH session access to the CPS appliance and specifies the SSH authentication method. When you enable SSH, all CPS sessions will be terminated if a CPS SSH server key must be generated. You must also have previously specified an authentication method other than None with the Server Security command.

If you enable plain text Telnet connections with a Server Security command, enabling SSH session access with the Server SSH command will add that as a valid connection method (both plain text and SSH connections will be allowed).

For more information, see *Connecting to devices using SSH* on page 16.

Access right: SCON
Access level: APPLIANCEADMIN

Syntax

SERVER SSH ENABLE|DISABLE [AUTH=<*auth*>]

Table 5.23: Server SSH Command Parameters

Parameter	Description
ENABLE|DISABLE	Enables or disables SSH session access to the CPS appliance.
AUTH=<*auth*>	SSH authentication methods. You must enter the entire value; abbreviations are not permitted. Valid values are: PW Password authentication. KEY Key authentication. PW|KEY Password or key authentication. KEY|PW Key or password authentication. PW&KEY Password and key authentication. KEY&PW Key and password authentication. Default = PW

Show Commands

The Show command has several forms, as listed in Table 5.24.

Table 5.24: Show Command Summary

Command	Description
Show Port	Displays configuration information and statistics for one or all ports.
Show Port Alert	Displays port alert strings.
Show Port In/Out	Displays how carriage returns and linefeeds are treated.
Show Server	Displays CPS configuration information and statistics.
Show Server CLI	Displays CPS CLI settings.
Show Server PPP	Displays CPS PPP settings.
Show Server RADIUS	Displays CPS RADIUS settings.
Show Server Security	Displays CPS authentication, connection and security lock-out settings.
Show Server SNMP	Displays SNMP configuration information.
Show User	Displays user configuration and session information.

Show Port command

The Show Port command displays configuration and status information about one or all ports.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW PORT [<*port*>|ALL|NAMES]

The SHOW PORT NAMES command display includes the port numbers and names. If a port has not been given a name with a Port Set command, the default name is displayed. A default name contains the last three octets of the MAC address plus the port number.

Table 5.25: Show Port Command Parameter

Parameter	Description
<*port*>	Either a port number in the range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance, ALL to display information about all ports or NAMES to display only port names. Default = your port

Table 5.26 and Table 5.27 list the display fields for a Show Port command that specifies one or all ports.

Table 5.26: Show Port Command Display Fields for Console Ports

Field	Content
Port	Port number.
Serial Port Settings	Comma-separated string of port values: baud rate, number of bits, parity, stop bits, flow control, socket number, time-out value and CLI access character (from Port Set command). The CLI character is preceded by POR CLI= if it was defined with a Port Set command or by SER CLI= if it was defined with a Server CLI command.
TX Bytes	Number of bytes transmitted.
RX Bytes	Number of bytes received.
Errors	Number of TX/RX parity and framing errors.
Power	Device power status, if monitoring is enabled. ON indicates the device is on, OFF indicates the device is off. If monitoring is disabled, this field is blank.
Toggle **	Toggle value (from Port Set command).
Power Signal **	Signal and state being monitored for device power status (from Port Set command).
Logical name **	Logical port name, which contains last three octets of MAC address plus the port number.
User *	Username (from User Add command).
Level *	User's access level (from User Add and User Set Access commands).
Access *	User's access rights (from User Add and User Set Access commands).
Duration *	Duration of user's session.

* Displayed only when the command specifies a single port that is currently being accessed.
** Displayed only when the command specifies a single port that is not being accessed.

Table 5.27: Show Port Command Display Fields for SPC Ports

Field	Content
Status	ONLINE indicates the SPC device is powered on, OFFLINE indicates the SPC device is powered off.
Version	SPC firmware version.
Sockets	Number of sockets on the SPC device.
Minload	Minimum load amp value (from SPC command).
Maxload	Maximum load amp value (from SPC command).

Table 5.27: Show Port Command Display Fields for SPC Ports (Continued)

Field	Content
Wake	Wakeup state for socket (from SPC command).
ON Min	Minimum On time (from SPC command).
OFF Min	Minimum Off time (from SPC command).

Show Port Alert command

The Show Port Alert command displays a port's alert strings.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW PORT <*port*> ALERT

Table 5.28: Show Port Alert Command Parameter

Parameter	Description
<*port*>	Port number in the range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance.

Show Port In|Out command

The Show Port In|Out command displays the translation settings for all ports. These translation settings indicate how carriage returns and linefeeds are treated in incoming and outgoing serial data.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW PORT IN|OUT

Show Server command

The Show Server command displays CPS appliance configuration information and statistics.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER

Table 5.29: Show Server Command Display Fields

Field	Content
Server	IP address (from initial configuration or Server Set command).

Table 5.29: Show Server Command Display Fields (Continued)

Field	Content
Mask	Subnet mask (from initial configuration or Server Set command).
Gateway	Gateway IP address (from initial configuration or Server Set command).
Up Time	Days, hours, minutes and seconds since unit was rebooted.
MAC	Ethernet MAC address.
S/N	Serial number.
Port	Port number.
Username	Username (from User Add command).
Duration	Duration of session.
Socket	Telnet socket number.
From Socket	Telnet client IP address with socket number in parentheses.
IP Input and Output	Network IP statistics, including number of packets delivered, discarded and fragments.
TCP	Network TCP statistics, including in segs, out segs, errors and retransmissions.
UDP	Network UDP statistics, including in, out, errors and no port events.
BOOT	BIOS/Bootstrap version, date and time.
APP	Application version that is running, plus its date and time.

Show Server CLI command

The Show Server CLI command displays the serial CLI settings.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER CLI

Table 5.30: Show Server CLI Command Display Fields

Field	Contents
CLI Port	Serial CLI port number and terminal type.
Access Character	Control character used to access CLI.
History	Indicates whether a port's history buffer content is displayed (auto) or not displayed (hold) when a user connects to the port, and whether the buffer content is cleared (clear) or kept (keep) when a session ends.

Table 5.30: Show Server CLI Command Display Fields (Continued)

Field	Contents
Connect	Indicates whether a valid user on the serial CLI port may use the Connect command.
Modeminit string	String used to initiate modem connections on the serial CLI port.
Server CLI Timeout	Session time-out value, shown in full minute or minute:second form (for example, 3m for 3 minutes, 3:30 for 3 minutes, 3 seconds.
Local authentication	Configured CLI port authentication setting (Enabled or Disabled).
Local preemption level	Preemption level to be used when authentication is disabled on the serial CLI port and that port's user attempts to connect to another serial port.

Show Server PPP command

The Show Server PPP command displays the current PPP settings that were configured with the Server PPP command.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER PPP

Show Server RADIUS command

The Show Server RADIUS command displays the current CPS RADIUS settings that were configured with the Server RADIUS command.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER RADIUS

Show Server Security command

The Show Server Security command displays the current authentication, connection and lock-out settings that were configured with the Server Security and Server SSH commands.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER SECURITY

Table 5.31: Show Server Security Command Display Fields

Field	Contents
Authentication	Configured authentication method(s). This includes the SSH authentication method configured with the Server SSH command (or the default value), regardless of whether SSH is enabled.
Encryption	Configured connection methods: None, SSH or both.
Lockout	Configured security lock-out state (Enabled or Disabled). If Enabled, the number of hours in the lock-out period is included.
DS Server IP #0	IP address of DSView software server number 0.
DS Server IP #1	IP address of DSView software server number 1.
DS Server IP #2	IP address of DSView software server number 2.
DS Server IP #3	IP address of DSView software server number 3.
Preauth Certs	Preauthentication certificates.
Fingerprint (Hex)	SSH key MD5 hash.
Fingerprint (BB)	SSH key bubble babble.
Ping Reply	Configured ping setting (Enabled or Disabled).

Show Server SNMP command

The Show Server SNMP command displays SNMP configuration information.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW SERVER SNMP

Show User command

The Show User command displays information about one or all users.

Access right: SMON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SHOW USER [<*username*>|ALL]

Table 5.32: Show User Command Parameter

Parameter	Description
<*username*>|ALL	Username or All, which requests a display of all defined users. Default: user currently logged in

The Show User command display for one user includes the information in the following table.

Table 5.33: Show User Command Display Fields

Field	Contents
User	Username.
Level	User's access level. If a level was not configured, access rights determine the level: Users with SCON access => APPLIANCEADMIN. Users with USER or PCON but not SCON => ADMIN. Otherwise, USER level is assigned.
Access	User's access rights and preemption level.
Locked	YES if user is locked-out, NO if not.
Last Login	System up time value when the user logged in.
Port	Serial port to which user is connected.
Username	Username.
Duration	Duration of user's session.
Socket	Telnet socket number.
From Socket	Telnet client IP address and socket number.

A Show User All command display includes the information in the following table.

Table 5.34: Show User All Command Display Fields

Field	Contents
User	Username.
Pass	YES if user has a password defined, NO if not.
Key	YES if user has an SSH key defined, NO if not.
Lock	YES if user is locked-out, NO if not.

Table 5.34: Show User All Command Display Fields (Continued)

Field	Contents
Level	User's access level. If a level was not configured, access rights determine the level: Users with SCON access => APPLIANCEADMIN. Users with USER or PCON but not SCON => ADMIN. Otherwise, USER level is assigned.
Access	User's access rights and preemption level.

SPC Command

The SPC command changes settings for an SPC device and its sockets.

NOTE: This command configures the port for use with the DSView software. For standalone use of the SPC device, this command should not be used, and the CPS port to which the SPC is attached should be configured as TD=Console.

Access right: SCON or PCON
Access level: ADMIN or APPLIANCEADMIN

Syntax

SPC <*port*>|ALL [MINLOAD=<*amps*>] [MAXLOAD=<*amps*>] [SOCKET <*socket*>|ALL] [WAKE=ON|OFF] [ONMIN=<*time*>] [OFFmin=<*time*>]

Table 5.35: SPC Command Parameters

Parameter	Description
<*port*>	Port number in range 1-8 for a CPS810 appliance or 1-16 for a CPS1610 appliance.
ALL	Indicates that the settings that follow should be applied to all ports configured as SPC.
MINLOAD=<*amps*>	Minimum load in amperes in the range 0-30. A 0 value indicates no minimum load. Default = 0
MAXLOAD=<*amps*>	Maximum load in amperes in the range 0-30. A 0 value indicates no maximum load. Default = 0
SOCKET <*socket*>|ALL	Either a socket number on the SPC or All, which indicates that the settings that follow should be applied to all sockets on the SPC.
WAKE=ON|OFF	State that the socket will enter when the SPC is powered up. Default = ON

Table 5.35: SPC Command Parameters (Continued)

Parameter	Description
ONMIN=<*time*>	Minimum amount of time that a socket will stay on before it may be turned off. The value may be specified with S for seconds, M for minutes or H for hour. Valid values are: 0S, 15S, 30S, 45S, 60S, 75S, 90S, 105S. 1M, 2M, 3M, 4M, 5M, 10M, 15M, 30M, 60M. 1H. Default = 0S
OFFMIN=<*time*>	Minimum amount of time that a socket will stay off before it may be turned on. The value may be specified with S for seconds, M for minutes or H for hour. Valid values are: 0S, 15S, 30S, 45S, 60S, 75S, 90S, 105S. 1M, 2M, 3M, 4M, 5M, 10M, 15M, 30M, 60M. 1H. Default = 0S

User Commands

The User command has several forms, as listed in Table 5.36.

Table 5.36: User Command Summary

Command	Description
User Add	Adds a new user to the user database.
User Delete	Deletes a user from the user database.
User Logout	Terminates a user's active session.
User Set	Changes a user's configuration information.
User Unlock	Unlocks a locked-out user.

User Add command

The User Add command adds a new user to the CPS user database. The user database holds a maximum of 64 user definitions. For more information, see *Managing User Accounts* on page 22 and *Access rights and levels* on page 23.

Access right: USER
Access level: ADMIN or APPLIANCEADMIN

Syntax

USER ADD <*username*> [PASSWORD=<*pwd*>] [SSHKEY=<*keyfile*>] [FTPIP=<*ftpadd*>] [KEY=<*sshkey*>] [ACCESS=<*access*>] [PREEMPT=1|2|3|4]

Table 5.37: User Add Command

Parameter	Description
<*username*>	3-16 alphanumeric character username. Usernames are case sensitive.
PASSWORD=<*pwd*>	3-16 alphanumeric character password. Passwords are case sensitive.
SSHKEY=<*keyfile*>	Name of uuencoded public key file on an FTP server. The maximum file size that may be received is 4K bytes. If this parameter is specified, you must also specify the FTPIP parameter.
FTPIP=<*ftpadd*>	FTP server's IP address. If this parameter is specified, you must also specify the SSHKEY parameter.
KEY=<*sshkey*>	Uuencoded SSH key.
ACCESS=<*access*>	Command and port access rights or level. You may specify multiple access rights, separated by commas, or a level. Valid values for access rights are: P<*n*> Access to the specified port number. P<*x-y*> Access to the specified range of ports. PALL Access to all ports. USER User configuration access rights. PCON Port configuration access rights. SCON Configuration access rights. SMON Monitor access rights. BREAK Can issue Port Break command. Valid values for access levels are: ADMIN PALL, USER, SMON, PCON and BREAK access rights. APPLIANCEADMIN PALL, USER, SCON, SMON, PCON and BREAK access rights. Default = PALL,SMON
PREEMPT=1|2|3|4	Preemption level, in the range 1(lowest) - 4 (highest). Default = 4 (highest)

Examples

The following command adds the username JohnDoe, with the password secretname, access to ports 2, 5, 6 and 7 and user and monitor access rights.

```
> user add JohnDoe password=secretname access=P2,5-7,user,smon
```

The following command adds the username JaneDoe, with access to all ports. The name of the SSH public user key file is cps_key2.pub. This file is located on the FTP server at IP address 10.0.0.3.

```
> user add JaneDoe ssh=cps_key2.pub ftp=10.0.0.3 access=pall
```

The following command adds the username JDoe and gives that user the Appliance Administrator access level, which enables access to all ports and CPS appliance commands.

```
> user add JDoe access=applianceadmin
```

User Delete command

The User Delete command removes a username entry from the CPS user database. The username may no longer be used to authenticate a session with the CPS appliance. If the specified user is currently logged in, a message is output to the user, indicating that access is no longer permitted, and the Telnet session is terminated.

Access right: USER
Access level: ADMIN or APPLIANCEADMIN

Syntax

USER DEL <*username*>

Table 5.38: User Delete Command Parameter

Parameter	Description
<*username*>	Username to be deleted.

User Logout command

The User Logout command terminates a user's active sessions on the CPS appliance. If the specified user has no active sessions, an error message is displayed. For all active sessions that are terminated, a message is sent to the Telnet client and the Telnet connection is dropped.

Access right: USER
Access level: ADMIN (may log out all except APPLIANCEADMIN) or APPLIANCEADMIN

Syntax

USER LOGOUT <*username*>

Table 5.39: User Logout Command Parameter

Parameter	Description
<username>	Username to be logged out.

User Set command

The User Set command changes a user's configuration in the user database. For more information, see *Managing User Accounts* on page 22 and *Access rights and levels* on page 23.

You may delete a user's password or key; however, each user must have a password or a key, so you cannot remove both. Also, you cannot remove a user's password or key if that action would result in no users having USER access rights.

Access right: none to change your own password, USER to change anything else;
Access level: none to change your own password, ADMIN or APPLIANCEADMIN to change anything else

Syntax

USER SET <*username*> [PASSWORD=<*pwd*>] [SSHKEY=<*keyfile*>] [FTPIP=<*ftpadd*>] [KEY=<*sshkey*>] [ACCESS=<*access*>] [PREEMPT=1|2|3|4]

Table 5.40: User Set Command Parameters

Parameter	Description
<*username*>	Username.
PASSWORD=<*pwd*>	New 3-16 alphanumeric character password. Passwords are case sensitive. This parameter is required when changing another user's password. The password is displayed on the screen. For security, clear your screen display after issuing this command. To delete a password, specify Password =“”.
SSHKEY=<*keyfile*>	Name of uuencoded public key file on an FTP server. The maximum file size that may be received is 4K bytes.
FTPIP=<*ftpadd*>	FTP server's IP address.
KEY=<*sshkey*>	Uuencoded SSH key. To delete an SSH key (whether it was originally specified with the SSHKEY and FTPIP parameters or with the KEY parameter), specify Key=“”.
ACCESS=<*access*>	Command and port access rights or level. You may specify multiple access rights, separated by commas, or a level. If specifying access rights, you may use one of three forms: ACCESS=<*access*> to specify all access rights. ACCESS=+<*access*> to specify only access rights to be added. ACCESS=–<*access*> to specify only access rights to be deleted. Valid values for access rights are: P<n> Access to the specified port number. P<x-y> Access to the specified range of ports. PALL Access to all ports. USER User configuration access rights. PCON Port configuration access rights. SCON Configuration access rights. SMON Monitor access rights. BREAK Can issue Port Break command. Valid values for access levels are: ADMIN PALL, USER, SMON, PCON and BREAK access rights. APPLIANCEADMIN PALL, USER, SCON, SMON, PCON and BREAK access rights. Default = PALL,SMON
PREEMPT=1|2|3|4|	Preemption level, in the range 1 (lowest) - 4 (highest). Default = 4 (highest)

Examples

The following command sets the access rights for JohnDoe, enabling access to all ports with configuration and monitoring access rights and specifying a preemption level of three.

```
>user set JohnDoe access=pall,scon,smon pre=3
```

The following command removes the server configuration access right for JohnDoe, and leaves other access rights intact.

```
> user set JohnDoe access=-SCON
```

The following command deletes the SSH key information for JohnDoe. The command will complete successfully only if JohnDoe has a password configured in a previous User Add or User Set command, and if there are other users with User access rights.

```
> user set key=""
```

User Unlock command

The User Unlock command unlocks a user who was previously locked-out. After this command completes, the user will be able to attempt login authentication again.

Access right: USER
Access level: ADMIN (may unlock all except APPLIANCEADMIN) or APPLIANCEADMIN

Syntax

USER UNLOCK <*username*>

Table 5.41: User Logout Command Parameter

Parameter	Description
<username>	Username to be unlocked.

APPENDICES

Appendix A: Technical Specifications

Table A.1: CPS 810/1610 Appliance Technical Specifications

Item	Value
Device Ports	
Number	8 (CPS810 appliance); 16 (CPS1610 appliance)
Type	Serial ports
Connectors	Serial port RJ-45
Network Connection	
Number	1
Type	Ethernet: IEEE 802.3, 10BaseT Fast Ethernet: IEEE 802.3U, 100BaseT
Connector	RJ-45
Dimensions	
H x W x D	4.45 x 22.23 x 20.32 cm 1U form factor (1.75 x 8.75 x 8.00 in)
Weight	5 lbs (2.3 kg) without cables
Heat Dissipation	75 BTU/hr (CPS810 appliance); 102 BTU/hr (CPS1610 appliance)
Airflow	2.5 cfm
Power Consumption	22 W (CPS810 appliance); 30 W (CPS1610 appliance)
AC-input power	50 W maximum
AC-input maximum	90 to 267 VAC
AC-input current rating	0.5 A
AC-input cable	18 AWG three-wire cable, with a three-lead IEC-320 receptacle on the power supply end and a country dependent plug on the power resource end
Frequency	50 to 60 Hz

Table A.1: CPS 810/1610 Appliance Technical Specifications (Continued)

Item	Value
Temperature	0° to 40° Celsius (32° to 104° Fahrenheit) operating -20° to +65° Celsius (-4° to +149° Fahrenheit) nonoperating
Humidity	10% to 90% noncondensing
Safety and EMC Standards	FCC P 15 Class A, EN55022, EN61000-3-2, EN61000-3-3, EN60950, EN55024, ETL (UL 1950), CSA 22.2 No. 950

Appendix B: Device Cabling

Each CPS appliance serial port has an RJ-45 connector for attaching a serial device. Table B.1 lists the pin assignments.

Table B.1: Port Pin Assignments

Pin Number	RS-232 Signal	Direction	Description
1	RTS	Output	Request to Send
2	DSR	Input	Data Set Ready
3	DCD	Input	Data Carrier Detect
4	RD	Input	Receive Data
5	TD	Output	Transmit Data
6	GND	(N/A)	Signal Ground
7	DTR	Output	Data Terminal Ready
8	CTS	Input	Clear to Send
NOTE: RI (Ring Indicate) is not supported			

Modular adaptors are available from Avocent to convert RJ-45 modular jacks to standard pinout configurations. Adaptors are available for use with:

- CAT 5 cable.
- Serial reversing cable. Reversing adaptors and cables are recommended for distances greater than 100 feet.

Adaptors for Use with CAT 5 Cable

Table B.2 lists the adaptors available from Avocent for use with CAT 5 cables.

Table B.2: Adaptors for Use with CAT 5 Cable

Part Number	Description
210122	RJ-45 to DB-9M (DTE) Adaptor
210120	RJ-45 to DB-9F (DCE) Adaptor
210124	RJ-45 to DB-25M (DTE) Adaptor
210123	RJ-45 to DB-25M (DCE) Adaptor
210125	RJ-45 to DB-25F (DTE) Adaptor
210121	RJ-45 to DB-25F (DCE) Adaptor

Table B.2: Adaptors for Use with CAT 5 Cable (Continued)

Part Number	Description
210127	RJ-45 to RJ-45 Male Adaptor for Cisco and Sun Netra console port
750238	CAT 5 Serial Starter Kit - includes all the above adaptors

Figure B.1 shows the pin assignments for the adaptors listed in Table B.2.

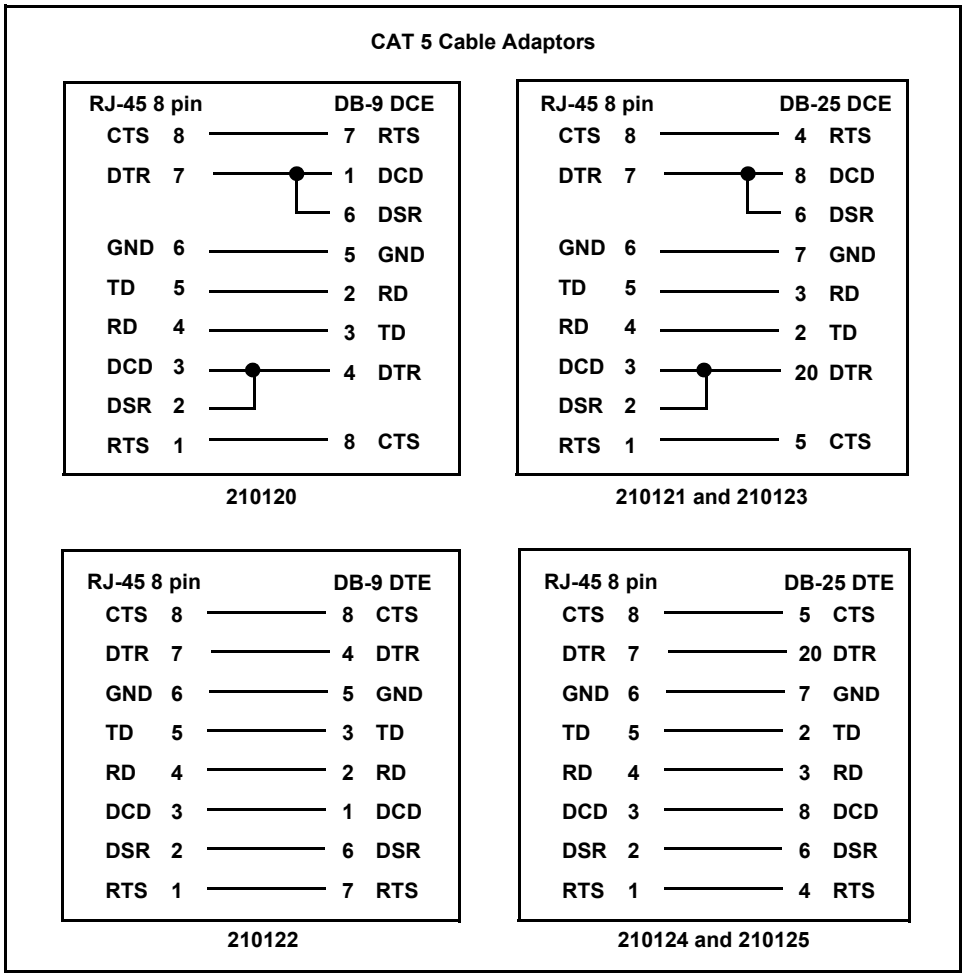


Figure B.1: CAT 5 Cable Adaptor Pin Assignments

Reversing Adaptors and Cables

Table B.3 lists the reversing adaptors and reversing cables available from Avocent.

Table B.3: Reversing Adaptors and Cables

Part Number	Description
210094	RJ-45 to DB-9M (DTE) Adaptor
210095	RJ-45 to DB-9F (DCE) Adaptor
210090	RJ-45 to DB-25M (DTE) Adaptor
210092	RJ-45 to DB-25M (DCE) Adaptor
210091	RJ-45 to DB-25F (DTE) Adaptor
210093	RJ-45 to DB-25F (DCE) Adaptor
210105	RJ-45 to RJ-45 Male Adaptor for Cisco and Sun Netra console port
690226	10 foot 8-wire Reversing Modular Cable
690227	25 foot 8-wire Reversing Modular Cable
690228	75 foot 8-wire Reversing Modular Cable
750122	Wiring Starter Kit (8-wire) - includes all the above adaptors and one 690226 cable

Figure B.2 shows the pin assignments for the adaptors listed in Table B.3.

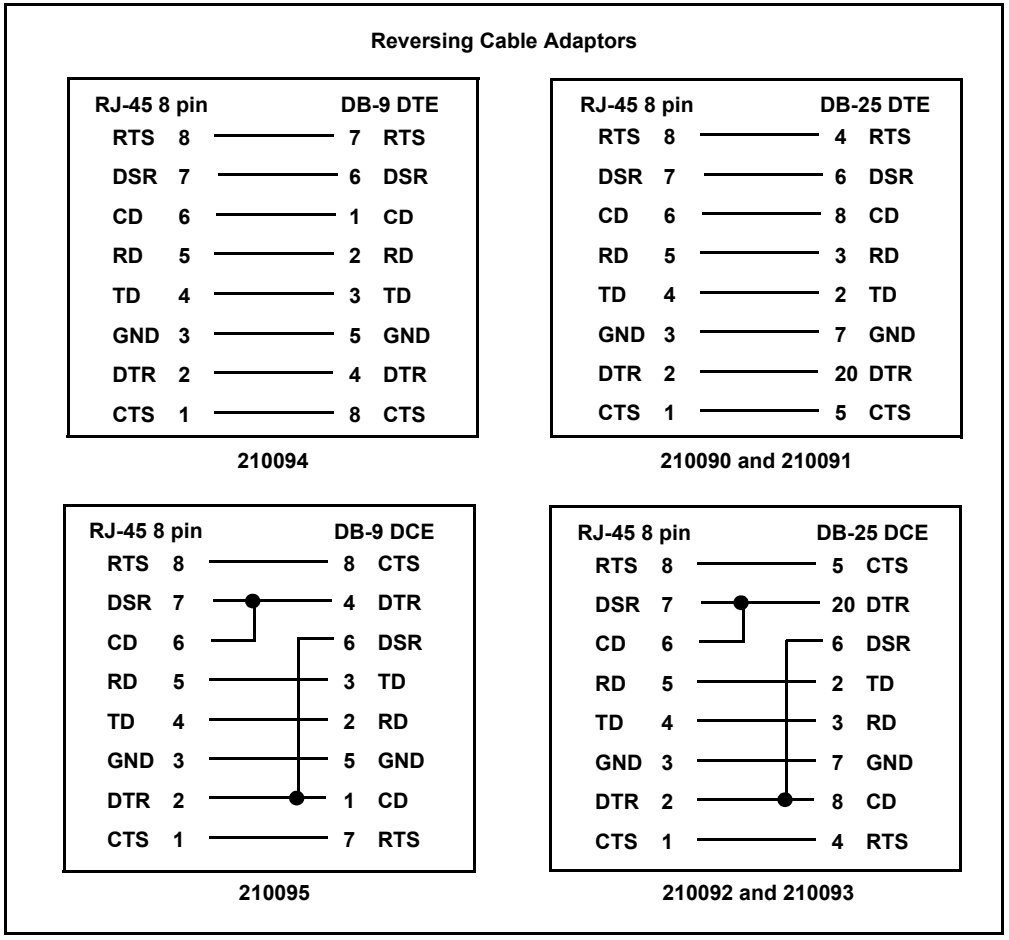


Figure B.2: Reversing Cable Adaptor Pin Assignments

If you choose to use a non-Avocent reversing cable, make sure the cable is reversing, as shown in Figure B.3.

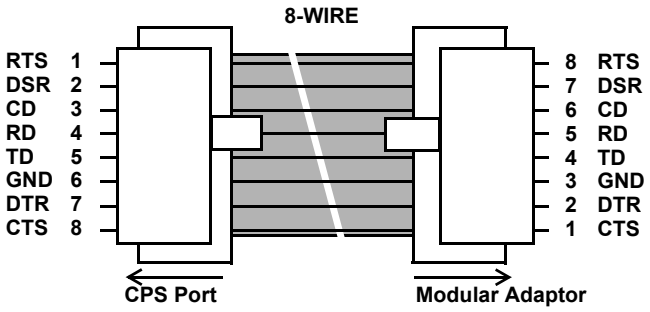


Figure B.3: 8-wire RJ-45 Reversing Cable

Appendix C: Supported Traps

The CPS appliance supports the following MIB2 traps:

- authenticationFailure
- linkUp
- linkDown
- coldStart

Table C.1 lists the supported enterprise traps. The Avocent web site, www.avocent.com, contains the complete trap MIB.

Table C.1: CPS Appliance Enterprise Traps

Trap	Description and Variable(s)
rebootStarted	The CPS appliance is rebooting. Variable: command issued by username
userLogin	A user logged in to the CPS appliance. Variable: username
userLogout	A user logged out of the CPS appliance. Variable: username.
serialSessionStarted	A serial session has started. Variables: username, server name and port number.
serialSessionStopped	A serial session has stopped. Variables: username, server name and port number.
serialSession Terminated	Another user has terminated a serial session. Variables: command issued by username, terminated username, server name and port number.
imageUpgradeStarted	The CPS appliance has started an image upgrade. Variables: command issued by username, image type (boot or application), new version number, current version number.
imageUpgradeResults	An image upgrade has ended. Variables: result, upgrade was initiated by username, upgrade image type (boot or application), upgrade version number and running version number. (If the upgrade was successful, the two version numbers will match.)
userAdded	A new user has been added to the CPS appliance user database. Variables: command issued by username and new username.
userDeleted	A user has been deleted from the CPS appliance user database. Variables: command issued by username and deleted username.
userModified	A user's definition has been modified in the CPS appliance user database. Variables: command issued by username and modified username.

Table C.1: CPS Appliance Enterprise Traps (Continued)

Trap	Description and Variable(s)
userAuthentication Failure	A user failed to authenticate with the CPS appliance. Variable: username.
factoryDefaultsSet	The CPS appliance has received a command to set itself to factory default values. (The appliance sends this trap after receiving the command, but before actually reverting to factory default values.)
portAlert	The CPS appliance detected a port alert string on a serial port. Variables: server name, port number and port alert string.
configurationFile Loaded	The CPS appliance has loaded a configuration file. This trap applies to DSView software. Variables: command issued by username and name of loaded file.
userDatabaseFile Loaded	The CPS appliance has loaded a user database file. This trap applies to DSView software. Variables: command issued by username and name of loaded file.
powerOnDetected	The CPS appliance detected that a port's power on/off control signal is in the state indicating power is on. This trap is sent upon initialization if the condition is detected. Subsequent traps are sent only if this signal changes state. Variables: server name and port number.
powerOffDetected	The CPS appliance detected that a port's power on/off control signal is in the state indicating power is off. This trap is sent upon initialization if the condition is detected. Subsequent traps are sent only if this signal changes state. Variables: server name and port number.
SPCOnline	An SPC device is online. This trap is sent upon initialization of the SPC device if it is online and responding. Subsequent traps are sent if the SPC device changes from offline to online. Variables: SPC location name and CPS appliance port number.
SPCOffline	An SPC device is offline. This trap is sent upon initialization of the SPC device if it is not responding. Subsequent traps are sent if the SPC device changes from online to offline. Variables: SPC location name and CPS appliance port number.
SPCLoginError	An SPC device has a login error. This occurs when the appliance is unable to log in to the SPC device using the username configured in the appliance. Variables: SPC location name, CPS appliance port number, username attempting to log in.
SPCSocketOn Command	The On command was issued to an SPC socket. Variables: command issued by username, server name, SPC location name, CPS appliance port number and SPC socket number.
SpcSocketOff Command	The Off command was issued to an SPC socket. Variables: command issued by username, server name, SPC location name, CPS appliance port number and SPC socket number.

Table C.1: CPS Appliance Enterprise Traps (Continued)

Trap	Description and Variable(s)
SPCSocketReboot Command	The Reboot command was issued to an SPC socket. Variables: command issued by username, server name, SPC location name, CPS appliance port number and SPC socket number.
SPCSocketOnSense Failure	An SPC socket encountered an on sense failure. Variables: server name, SPC location name, CPS appliance port number and SPC socket number.
SPCSocketOffSense Failure	An SPC socket encountered an off sense failure. Variables: server name, SPC location name, CPS appliance port number and SPC socket number.
SPCTotalLoadHigh	The SPC device has exceeded the total load maximum threshold. Variables: SPC location name and CPS appliance port number.
SPCTotalLoadLow	The SPC device exceeded the total load minimum load threshold. Variables: SPC location name and CPS appliance port number.
SPCSocketStatusOn	An SPC socket's state changed to 'on.' Variables: server name, SPC location name, CPS appliance port number and SPC socket number.
SPCSocketStatusOff	An SPC socket's state changed to 'off.' Variables: server name, SPC location name, CPS appliance port number and SPC socket number.
userLocked	A user account has been locked. Variables: client IP address, locked username and reason.
userUnlocked	A user account has been unlocked. Variables: client IP address, command issued by username, unlocked username and reason.
aggregatedServer StatusChg	The status of one or more servers (connections paths) has changed. The appliance always sends this trap upon bootup. Thereafter, it sends the trap when there is a change in connection path status, and will include only those paths whose status has changed. Variable(s): connection path(s)

Appendix D: Ports Used

Table D.1 lists the UDP and TCP port numbers used by the CPS appliance. The values assume a default configuration; some values are configurable.

Table D.1: Ports Used by CPS Appliance

Port Type and Number	Used for
TCP 22	SSH2, if enabled.
TCP 23	Telnet.
UDP 161	SNMP, if enabled.
TCP 3211	Secure protocol used by DSView software.
TCP 3001-3016	Telnet serial sessions with ports 1-16.
TCP 3101-3116	SSH serial sessions with ports 1-16.
TCP 3871	Secure protocol used by DSView software.

Appendix E: Technical Support

Our Technical Support staff is ready to assist you with any installation or operating problems you encounter with your Avocent product. If an issue should develop, follow the steps below for the fastest possible service:

1. Check the pertinent section of the manual to see if the issue can be resolved by following the procedures outlined.
2. Check our web site at www.avocent.com/support to search the knowledge base or use the on-line service request.
3. Call Avocent Technical Support for assistance at (888) 793-8763. Visit the Avocent web site at http://www.avocent.com/support and click on *Support Phone Numbers* for current phone support hours.

INDEX

A

Access rights and levels
- about 23
- changing 24
- configuring 24
- displaying 24

Adaptors 77
Authentication
- configuring 26, 57
- displaying configuration information 27, 66
- summary 26
- types 24
- using DSView software 24, 57
- See also *RADIUS*

B

BootP 7
Buttons 5

C

Cabling 77
CLI
- accessing 35
- changing the access character 20, 47, 51
- displaying access character 65
- displaying the access character 20
- mode (Telnet CLI) 20

CLI port
- configuring 14, 51
- connecting to device from 14
- displaying configuration information 14

Commands
- Connect 43
- conventions 36
- Disconnect 43
- Help 44
- line editing for ASCII TTY devices 36
- line editing for VT100 compatible devices 35
- Port Alert Add 45
- Port Alert Copy 45
- Port Alert Delete 46
- Port Break 46
- Port command summary 44
- Port History 46
- Port Logout 47
- Port Set 47
- Port Set In/Out 49
- Quit 50
- Resume 50
- Server CLI 51
- Server command summary 51
- Server FLASH 53
- Server PPP 54
- Server RADIUS 55
- Server Reboot 56
- Server Security 57
- Server Set 57
- Server SNMP 58
- Server SNMP Community 58
- Server SNMP Manager 59
- Server SNMP Trap 59
- Server SNMP Trap Destination 60
- Server SSH 61
- Show command summary 62
- Show Port 62
- Show Port Alert 64
- Show Port In/Out 64

Show Server 64
Show Server CLI 65
Show Server PPP 66
Show Server RADIUS 66
Show Server Security 66
Show Server SNMP 67
Show User 67
SPC 69
summary 38
syntax 36
User Add 70
User command summary 70
User Delete 72
User Logout 72
User Set 72
User Unlock 74
Configuration
IP address and subnet mask 7
serial port settings 12
See also *Port*
Connect command 43
Conventions in commands 36

D

Device cabling 77
Device connection methods
about 13
dial-in 15
ending device sessions 20
from serial CLI port 14
preemption 21
session time-out 21
using PPP 15
using SSH 16
using Telnet 13
Dial-in connections
about 15
displaying configuration information 15, 65
specifying modem initialization string 15, 51
Disconnect command 43
DSView software
authentication using 24, 57
clearing stored credentials 57
configuring network addresses using 7
connecting to devices 13
using 3

E

Encryption
configuring 57
displaying configuration information 66

F

FLASH updating 53

G

Gateway
changing 57
configuring 7
displaying 64

H

Hardware installation 6
Help command 44
History buffer
about 28
accessing port history mode 29, 46
clearing and discarding contents 30
commands in history mode 28
controlling content when session ends 30, 51
controlling display at connection 29, 51

displaying configuration information 65

I

Initial login 9
Installation
configuring addresses 7
hardware 6
IP address
changing 57
configuring 7
displaying 64

L

LEDs 5
Line editing operations
ASCII TTY devices 36
VT100 compatible devices 35
Lock-out. See *Security lock-out*
Login 9
Logout 47, 72

M

Modem. See *Dial-in connections*
Modular adaptors 77

P

Port
command summary 44
configuring settings 12
default settings 11
displaying settings 12, 62
pin assignments 77
session time-out 21
See also *History buffer* and *SNMP*
Port Alert Add command 45
Port Alert Copy command 45
Port Alert Delete command 46
Port alert strings. See *SNMP*
Port Break command 46
Port History command 46
Port Logout command 47
Port Set command 47
Port Set In/Out command 49
Ports used by appliance 85
PPP
about 15
displaying configuration information 16, 66
enabling/disabling server 16, 54
Preemption 21

Q

Quit command 50

R

RADIUS
about 25
configuring 26, 55, 57
displaying configuration information 27, 66
Reinitialization 10
Resume command 50

S

Security lock-out
about 27
enabling/disabling 28, 57
unlocking a user 28, 74
Server CLI command 51
Server command summary 51
Server FLASH command 53
Server PPP command 54
Server RADIUS command 55

Server Reboot command 56
Server Security command 57
Server Set command 57
Server SNMP command 58
Server SNMP Community command 58
Server SNMP Manager command 59
Server SNMP Trap command 59
Server SNMP Trap Destination command 60
Server SSH command 61
Session
ending 20, 47, 50, 72
preemption 21
time-out 21, 47, 51, 65
Show command summary 62
Show Port Alert command 64
Show Port command 62
Show Port In/Out command 64
Show Server CLI command 65
Show Server command 64
Show Server PPP command 66
Show Server RADIUS command 66
Show Server Security command 66
Show Server SNMP command 67
Show User command 67
SNMP
about 30
adding port alert strings 32, 45
adding/deleting management addresses 31
adding/deleting trap destination addresses 60
adding/deleting trap destinations 32
copying port alert strings 32, 45
deleting port alert strings 32, 46
displaying configuration information 33, 67
displaying port alert string information 33, 64
enabling/disabling 30, 58
enabling/disabling traps 31, 59
specifying community names 31, 58
specifying management entity addresses 59
SPC command 69
SPC device
configuring ports and settings 12, 69
displaying configuration information 12, 62
SSH
about 16
authenticating users 17
disabling access 19, 61
displaying configuration information 19, 66
enabling access 19, 61
server keys 17
user keys 18
Statistics
network 64
port 62
Subnet mask
changing 57
configuring 7
displaying 64

T

Technical
specifications 75
support 86
Telnet
CLI mode 20
connections to devices 13
Time-out. See *Session time-out*
Traps 82

U

User accounts

access rights and levels 23
adding 22, 70
changing 22, 72
deleting 23, 72
displaying 23, 67
User Add command 70
User command summary 70
User Delete command 72
User Logout command 72
User Set command 72
User Unlock command 74

LIMITED WARRANTY

Avocent Corporation warrants to the original retail purchaser that this product is and will be free from defects in materials and workmanship for a period of 24 months from the date of purchase.

Additionally, all Avocent products carry an unconditional thirty-day satisfaction guarantee. If, for any reason, you are dissatisfied with the performance of this product, you may return it to the point of purchase for a refund of the purchase price (excluding shipping charges). This guarantee does not apply to special order products, and may not be available through all resellers. During the warranty period, purchaser must promptly call Avocent for a RETURN MATERIALS AUTHORIZATION (RMA) number. Make sure that the RMA number appears on the packing slip, proof of purchase, AND ON THE OUTSIDE OF EACH SHIPPING CARTON. Unauthorized returns or collect shipments will be refused.

Ship prepaid to: Avocent Corporation
4991 Corporate Drive
Huntsville, AL 35805 U.S.A.
Telephone: (256) 430-4000

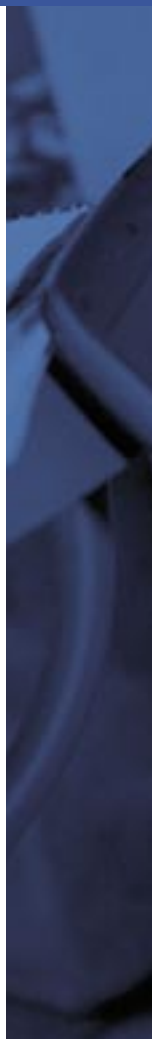
The above limited warranty is voided by occurrence of any of the following events, upon which the product is provided as is, with all faults, and with all disclaimers of warranty identified below:

1. If defect or malfunction was caused by abuse, mishandling, unauthorized repair, or use other than intended.
2. If unauthorized modifications were made to product.
3. If unreported damages occurred in any shipment of the product.
4. If damages were due to or caused by equipment or software not provided by Avocent.
5. If the unit is used with non-grounded or incorrectly polarized AC power.
6. If the product is used in contradiction to any instruction provided by any User Guide or Instruction Sheet provided to you or with the product.
7. If the product is damaged due to power surges, water exposure or act of God including lightning.

EXCEPT AS SPECIFICALLY PROVIDED ABOVE AND TO THE MAXIMUM EXTENT ALLOWED BY LAW, AVOCENT CORPORATION DISCLAIMS ALL WARRANTIES AND CONDITIONS WHETHER EXPRESS, IMPLIED, OR STATUTORY AS TO ANY MATTER WHATSOEVER INCLUDING, WITHOUT LIMITATION, TITLE, NON-INFRINGEMENT, CONDITION, MERCHANTABILITY OR FITNESS FOR ANY PARTICULAR OR INTENDED PURPOSE.

EXCEPT AS EXPRESSLY PROVIDED ABOVE AND TO THE MAXIMUM EXTENT ALLOWED BY LAW, AVOCENT CORPORATION SHALL NOT BE LIABLE FOR ANY SPECIAL, INDIRECT OR CONSEQUENTIAL DAMAGES (INCLUDING WITHOUT LIMITATION, LOSS OF PROFIT, LOSS OF BUSINESS, LOSS OF INFORMATION, FINANCIAL LOSS, PERSONAL INJURY, LOSS OF PRIVACY OR NEGLIGENCE) WHICH MAY BE CAUSED BY OR RELATED TO, DIRECTLY OR INDIRECTLY, THE USE OF A PRODUCT OR SERVICE, THE INABILITY TO USE A PRODUCT OR SERVICE, INADEQUACY OF A PRODUCT OR SERVICE FOR ANY PURPOSE OR USE THEREOF OR BY ANY DEFECT OR DEFICIENCY THEREIN EVEN IF AVOCENT CORPORATION OR AN AUTHORIZED AVOCENT DEALER HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES OR LOSSES.

Avocent
The Power of Being There



For Technical Support:

Email: support@avocent.com
www.avocent.com

Avocent Corporation
4991 Corporate Drive
Huntsville, Alabama 35805-6201 USA
Tel: +1 256 430 4000
Fax: +1 256 430 4031

Avocent International Ltd.
Avocent House, Shannon Free Zone
Shannon, County Clare, Ireland
Tel: +353 61 715 292
Fax: +353 61 471 871

Avocent Asia Pacific
Singapore Branch Office
100 Tras Street, #15-01
Amara Corporate Tower
Singapore 079027
Tel: +656 227 3773
Fax: +656 223 9155

Avocent Germany
Gottlieb-Daimler-Straße 2-4
D-33803 Steinhagen
Germany
Tel: +49 5204 9134 0
Fax: +49 5204 9134 99

Avocent Canada
50 Mural Street, Unit 5
Richmond Hill, Ontario
L4B 1E4 Canada
Tel: +1 877 992 9239
Fax: +1 877 524 2985

590-187-001H